

# Uygulamalı Rehberler

Her bir Uygulamalı Rehber belirli bir ücretsiz yazılım ya da açık kaynak yazılım aracının nasıl kullanılacağını açıklar. Potansiyel zorluklara değinir, yararlı öneriler verir ve en önemlisi araçları güvenli bir şekilde kullanmanız ve yapılandırmanız için size yol gösterir. Daha kolay takip edebilmeniz için ekran görüntüleri ve adım adım yönergeler içerir.

Bahsi geçen yazılımlar direkt ilgili Uygulamalı Rehberler'den ya da aracı geliştirenlerin websitelerinden ücretsiz indirilebilir. Çoğu zaman, bir aracı açıklayan rehberin hemen başlangıcında bulunan ilgili linki tıklayarak ve sonrasında tarayıcınıza kurucu programı Açmasını ya da Çalıştırmasını söyleyerek o aracı kurabilirsiniz. Bir Uygulamalı Rehber özel bir kurulum yönergesi verecek olursa, o aracı kurabilmek için dosyayı Masaüstü'nüze ya da başka bir klasöre kaydetmeniz gerekebilir.

Güvenliğiniz için, bu araçların en güncel sürümlerini kullanmaya çalışmalısınız. Bazı araçların şu anki sürümleri, ilgili Uygulamalı Rehberler oluşturulurken var olan sürümlerinden daha güncel olabilir. Bu gibi durumlarda, araçların kullanıcı arayüzleri Rehber'de görünenden biraz farklı olabilir.

Uygulamalı Rehberler, birkaç önemli Security-in-a-box aracının var olan taşınabilir sürümlerini de içerir. Bu sürümler direkt bir USB bellek çubuğuna çıkartılmak üzere tasarlanmıştır ki bunları istediğiniz herhangi bir bilgisayardan kullanabilesiniz. Taşınabilir araçlar yerel bir bilgisayara kurulmadığı için, onların varlıkları ve kullanımları saptanamaz. Ama, aklınızda bulundurun ki harici cihazınız, USB bellek çubuğunuz ve genel olarak tüm taşınabilir araçlar ancak kullandığınız bilgisayar kadar güvenlidir; reklam destekli yazılım, kötü niyetli yazılım, casus yazılım ve virüs tehlikelerine bilgisayarınız kadar açıktır.

## KeePass - Güvenli Şifre Muhafazası

### Short Description:

**KeePass** güvenli ve kullanımı kolay bir şifre yönetimi aracıdır.

### Online Installation Instructions:

#### KeePass'i indirme

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Keepass** ikonunu **tıklayarak** [www.keepass.info/download.html](http://www.keepass.info/download.html) sayfasını açın
- Sayfanın **Classic Edition** kısmındaki "**KeePass 1.xx (Installer EXE for Windows)**"u tıklayın
- **KeePass-1.xx-Setup.exe** dosyasını kaydedin, bulup üzerine çift tıklayın
- **KeePass'** başarıyla kurduktan sonra kurucu programı bilgisayarınızdan silebilirsiniz.

#### Keepass:



<sup>[2]</sup>

#### Homepage

[www.keepass.info](http://www.keepass.info) <sup>[3]</sup>

#### Bilgisayar Gereksinimleri

- Tüm Windows versiyonları

#### Bu rehberde kullanılan sürüm

- 1.27

#### Bu bölümün son güncellenme tarihi

- Temmuz 2014

#### Lisans

- Özgür ve Açık-Kaynak Yazılım

#### Gerekli Okuma

- Nasıl Yapmalı Kitapçığının 3. Bölümü, Güvenli şifreler nasıl oluşturulur ve muhafaza edilir [4]

#### Buradan sağlayacağınız faydalar:

- Tüm şifrelerinizi tek bir güvenli ve kullanımı kolay veri tabanında saklayabilmek
- Aklınızda tutmanızı gerektirmeden, istediğiniz sayıda güçlü şifre yaratmak ve onları saklayabilmek

#### GNU Linux, Mac ve Microsoft Windows'a Uyumlu Diğer Programlar:

KeePass aynı zamanda GNU Linux ve Mac OS (KeePassX [5] sürümü) kullanılabilir. KeePass'in çeşitli versiyonlarını, iPhone, BlackBerry, Android, ve PocketPC gibi başka platformlarda da bulabilirsiniz. Fakat başka programlar kullanmak istiyorsanız, sizlere aşağıdakileri önerebiliriz:

- **Password Safe** [6] Microsoft Windows ve GNU Linux'ta kullanılabilir.
- **1Password** [7] Mac OS, Microsoft Windows, iPhone and iPad'de kullanılabilir.

### 1.1 Başlamadan önce bu araç hakkında bilmeniz gerekenler

KeePass, tüm şifrelerinizi yüksek güvenilirlikli bir veri tabanında saklamanızı sağlayan, kullanımı kolay ve güçlü bir araçtır. Bu veri tabanını ve KeePass programını bir USB hafıza çubuğuna koyarak yanınızda taşıyabilirsiniz. Bu veri tabanı yaratacağınız bir 'ana şifre' ile korunur. Bu şifre aynı zamanda veri tabanınızın içeriğinin şifresini çözmek için de kullanılır. Var olan şifrelerinizi KeePass'te saklayabilir veya KeePass'in sizin için şifre oluşturmasını isteyebilirsiniz. KeePass herhangi bir önceden yapılandırma veya özel kurulum yönergeleri gerektirmez. Siz hazır olduğunuz anda kullanıma hazırdır!

#### Offline Installation Instructions :

##### KeePass'i İndirme

- Kısa **Uygulamalı Rehberler'in** [1] Giriş bölümünü okuyun
- Aşağıdaki **Keepass** ikonunu **tıklayıp** kurucuyu 'Açın' ya da 'Çalıştırın'. Gerekirse kurucuyu ilk önce kaydedin ve sonrasında bulup üzerine çift tıklayın.
- Devam etmeden önce bir sonraki kısımdaki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz, kurulumdan sonra silebilirsiniz

KeePass:



[8]

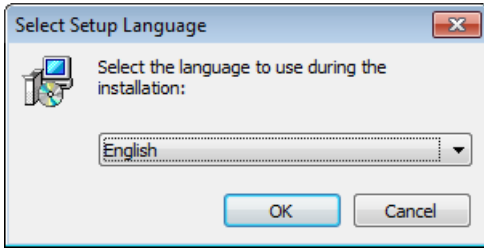
## KeePass Nasıl Kurulur ve Kullanılır

Bu sayfadaki kısımların listesi:

- **2.0 KeePass Nasıl Kurulur**
- **2.1 Keepass Arayüzü Nasıl Türkçe'ye Çevrilir**
- **2.2 Yeni Bir Parola Veritabanı Nasıl Oluşturulur**
- **2.3 Nasıl Kayıt Eklenir**
- **2.4 Bir Kayıt Nasıl Düzenlenir**
- **2.5 Rastgele Parolalar Nasıl Üretilir**
- **2.6 KeePass Nasıl Küçültülür, Keepass'ten Nasıl Çıkılır**
- **2.7 Parola Veritabanı Dosyası Nasıl Yedeklenir**
- **2.8 Temel Anahtar Nasıl Yeniden Tanımlanır**

### 2.0 KeePass Nasıl Kurulur

1. Adım.  KeePass-1.29-Setup'a çift tıklayın, Dosya Aç-Güvenlik Uyarısı iletişim kutusu açılabilir. Açılırsa, 'ı tıklayın ve aşağıda görünen ekranı etkinleştirin:



Şekil 1: Kurulum Dilini Seçin ekranı

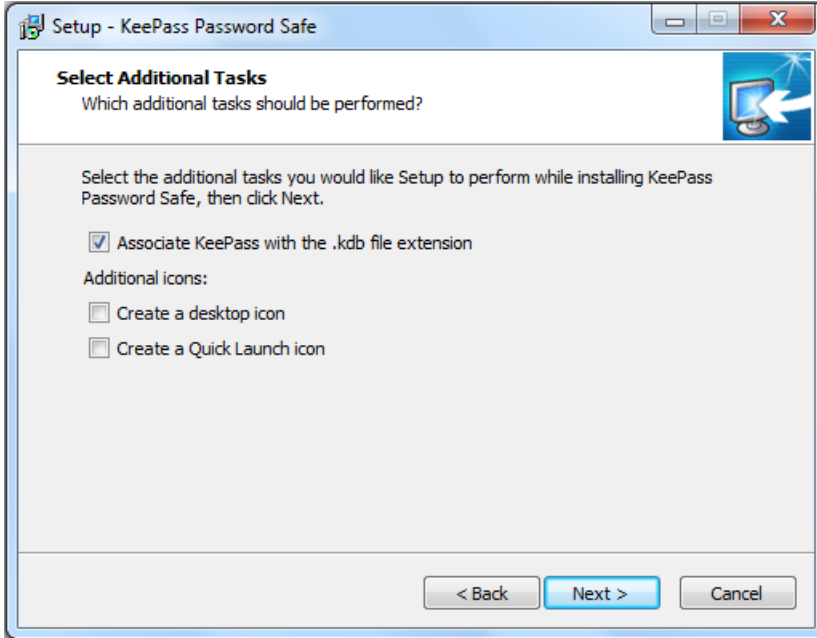
**2. Adım.** 'ı tıklayarak Kur – KeePass Parola Güvenliği - KeePass Parola Güvenliği Kurulum Sihirbazına Hoş geldiniz ekranını etkinleştirin.

**3. Adım.** Lisans Anlaşması ekranını etkinleştirmek için 'ı **tıklayın**. Kurulumla devam etmeden önce lütfen *Lisans Anlaşması'nı* okuyun.

**4. Adım.** *I accept the agreement'u işaretleyin* ve *Next* düğmesini etkinleştirin. 'ı **tıklayın** ve *Hedef Dosyayı Seç* ekranını etkinleştirin.

**5. Adım.** Verili kurulum yolunu kabul etmek için 'ı **tıklayın**.

**6. Adım.** Aşağıda görünen ekranı etkinleştirmek için 'ı **tıklayın**.



Şekil 2: Ek Komutları Seç ekranı

**7. Adım.** Yukarıdaki Şekil 2'de görüldüğü gibi ☒ Associate KeePass with the .kdb file extension seçeneğini **işaretleyin**.

**Not:** *Başlangıç Menüsü Dosyası Oluştur* seçeneğini işaretlerseniz, Kur – KeePass Parola Güvenliği kurulum sihirbazı, *Başlangıç* menüsünde otomatik olarak **KeePass Hızlı Başlat** iconu yaratacaktır.

**8. Adım.** Kurulum için Hazır özet bilgi ekranını başlatmak için 'ı **tıklayın**. **Kuruluyor** ekranını ve durum ilerleme çubuğunu etkinleştirmek için 'ı **tıklayın**.

Birkaç saniye sonra KeePass Parola Güvenliği Kurulum Sihirbazını Tamamlıyor ekranı görünecektir.

**9. Adım.** KeePass'i Başlat seçeneğini **tıklayın** ve ardından 'ı **tıklayın**. Bunu yaptığınız zaman, eğer İnternet bağlantınız varsa, **KeePass** anında açılacaktır ve sizi **KeePass Uzantı ve Eklentiler** websitesine yönlendirecektir.

## 2.1 KeePass Arayüzü Nasıl Türkçe'ye Çevrilir

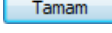
KeePass arayüzünü Türkçe'ye çevirmek için aşağıdaki adımları uygulayın:

**1. Adım.** <http://keepass.info/translations.html>'ye <sup>[9]</sup> tıklayarak KeePass Çeviriler sayfasına ulaşın.

**2. Adım.** Sayfayı aşağı **kaydırarak** çeviri listesinin sonralarına doğru göreceğiniz  **Turkish** simgesiyle aynı hizada

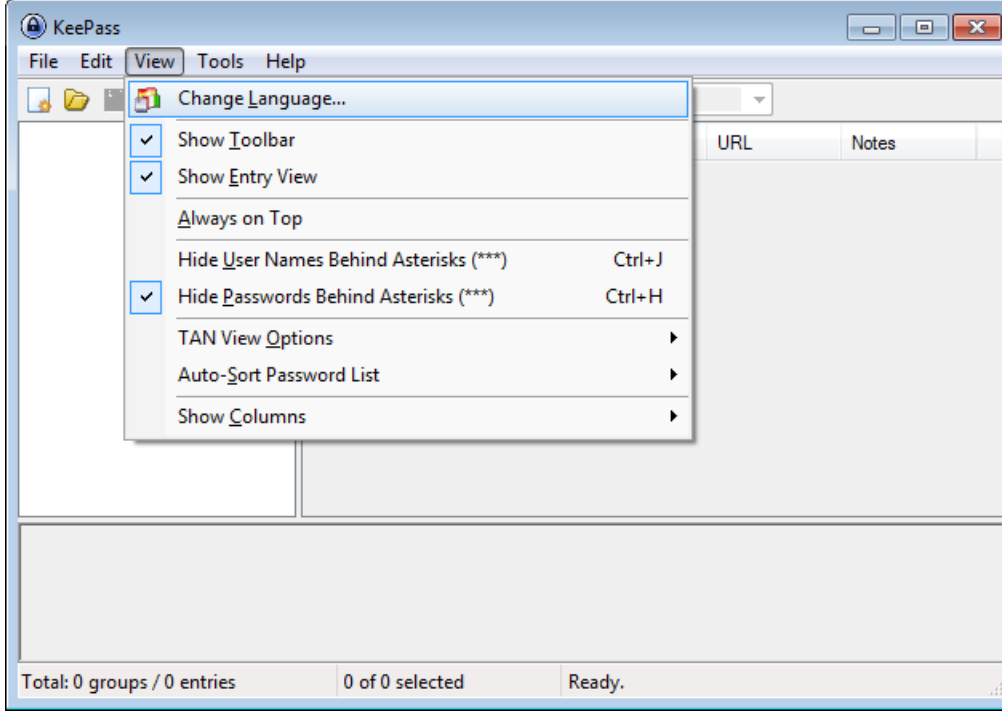
olan  [1.29+] simgesine **tıklayın**. Bu arayüz çeviri dosyasını bilgisayarınıza kaydecektir.

**3. Adım.** İndirdiğiniz sıkıştırılmış  KeePass-1.29-Turkish dosyasını **bulup** üzerine **sağ tıklayın** ve **Tümünü Ayıkla...** seçeneğini seçin.

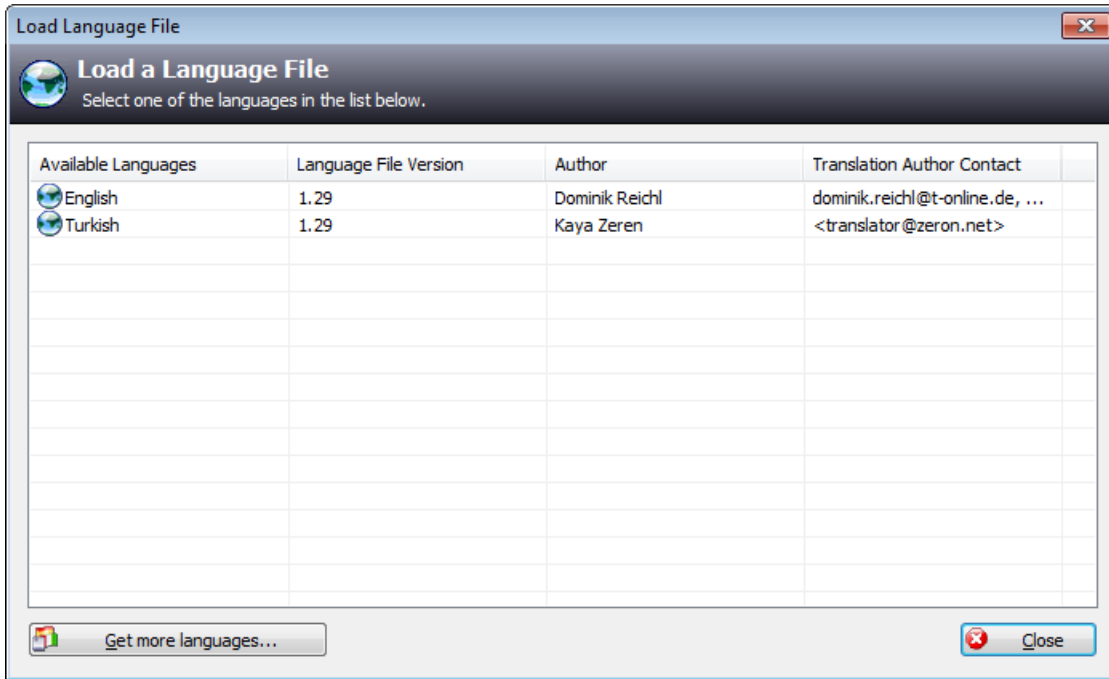
**4. Adım.** Ardından açılan ekranda 'ı **tıklayın** ve **Keepass.exe** dosyasının bulunduğu klasöre (C:\Program Files (x86)\KeePass Password Safe gibi) ilerleyin. 'ı tıklayın.

**5. Adım.** 'yı tıklayın. Bu sayede klasörde  Turkish.lng dosyası belirecektir.

**6. Adım.** **Keepass'i** açın. *Şekil 4'te* görüldüğü gibi **View > Change Language...** seçeneğini **tıklayın**. Bu *Dil Dosyasını Yükle* ekranını (*Şekil 5*) açacaktır.

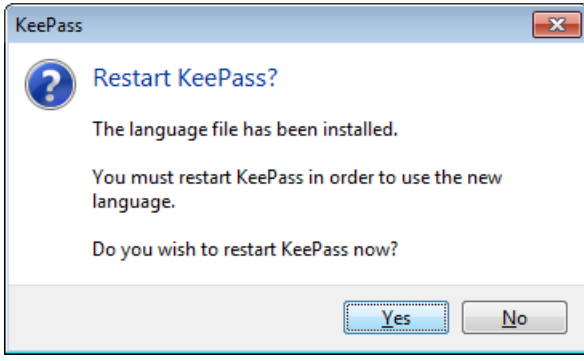


*Şekil 4: Keepass İngilizce arayüzünde Arayüz dilini değiştirme seçeneği*

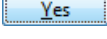


*Şekil 5: Keepass İngilizce arayüzünde elde olan çevirilerin listesi*

**7. Adım.** **Turkish** seçeneğine **çift tıklayıp** aşağıdaki ekranı etkinleştirin.



Şekil 6: KeePass İngilizce arayüzünde dil geçişinin tamamlanması için programın yeniden başlatılması gerektiği uyarısını veren diyalog ekranı

**8. Adım.** Türkçe arayüzün etkinleştirilebilmesi için **Keepass**'in yeniden başlatılması gerekir. 'i tıklayın.

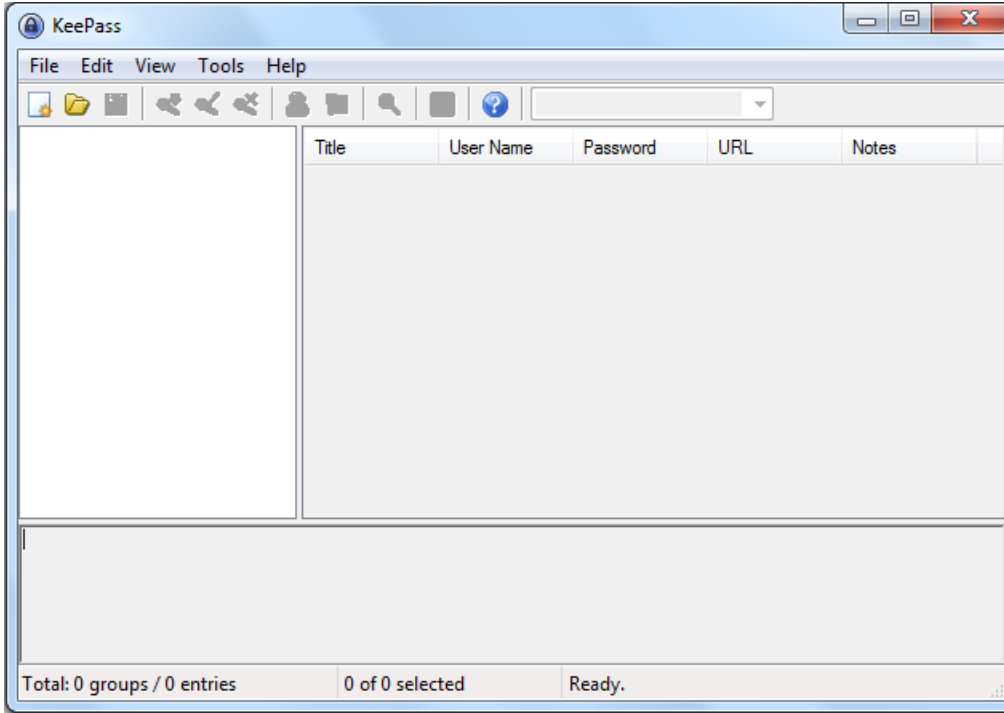
**Keepass** Tekrar açıldığında dili Türkçe olacaktır.

## 2.2 Yeni Bir Parola Veritabanı Nasıl Oluşturulur

Takip eden kısımlarda nasıl temel parola üretebileceğinizi, yeni yaratılan veritabanınızı nasıl kaydedebileceğinizi, bir program için rastgele bir parolayı nasıl kurabileceğinizi, bir veritabanını nasıl yedekleyebileceğinizi ve **Keepass**'teki parolaları nasıl kullanıma sokabileceğinizi öğreneceksiniz.

**KeePass**'i başlatmak için aşağıdaki adımları takip edin:

**1. Adım. KeePass** ana ekranını aşağıda görüldüğü gibi etkinleştirmek için **Başlat > Tüm Programlar > KeePass**'i seçin veya masa üstünüzdeki  ikonuna tıklayın.



Şekil 7: KeePass Parola Güvenliği konsolu

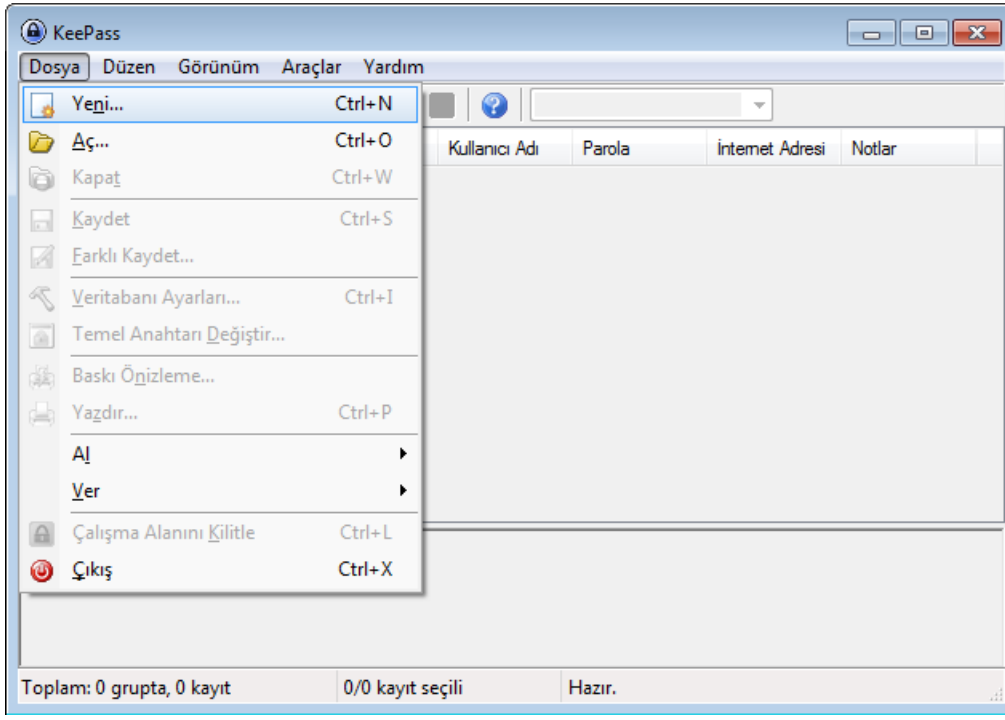
### 2.1.1 Yeni Bir Parola Veritabanı Nasıl Oluşturulur

Yeni bir parola veri tabanı oluşturmak iki adımdan oluşur:

Parola veri tabanınızı kilitlemek ve kilidini açmak için orijinal ve güçlü bir temel parola oluşturmalısınız. Ardından bu veri tabanı parolasını kaydetmelisiniz.

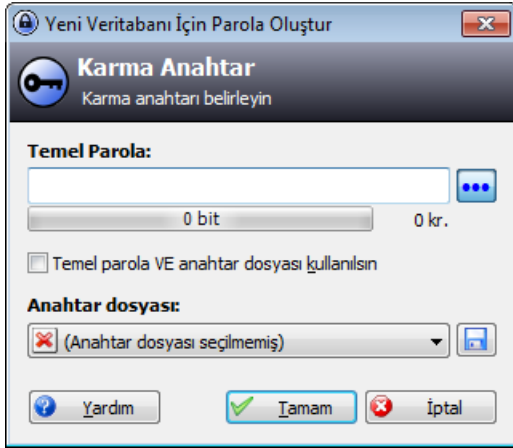
Yeni bir veri tabanı parolası oluşturmak için şu adımları takip edin:

**1. Adım. Dosya > Yeni**'yi aşağıdaki gibi seçin :



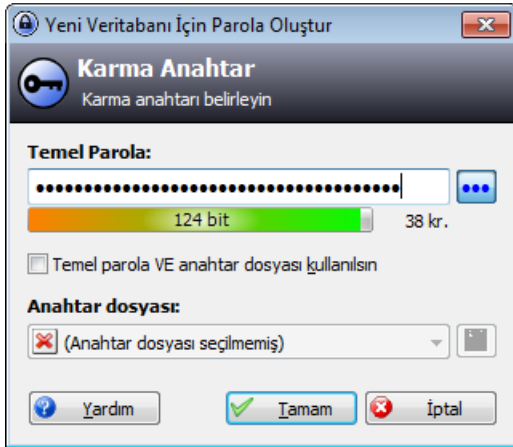
Şekil 8: Dosya > Yeni seçili KeePass ekranı

Bu şekilde Yeni Parola Veritabanı Oluştur ekranı aşağıda görüldüğü gibi etkinleşir:



Şekil 9: KeePass Yeni Parola Veritabanı Oluştur ekranı

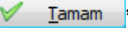
**2. Adım.** Yeni oluşturduğunuz temel parolayı *Temel Parola* kutucuğuna girin.

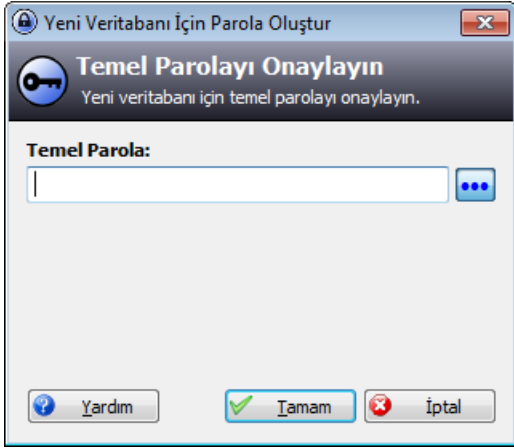


Şekil 10: Temel Parola alanı doldurulmuş Oluşturulmuş KeePass Ana Karma Anahtar Belirleyin ekranı

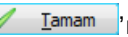
Parola alanının altında turuncu ve yeşil renklerinde bir ilerleme çubuğu göreceksiniz. Parolanızı girerken, karakterler çoğaldıkça bu çubuk üzerindeki yeşil rengi artacak ve böylelikle size Parolanızın karmaşıklığını ve gücünü gösterecek.

**İpucu:** Parolanızı girmeyi bitirdiğiniz zaman çubuğun en az yarısının yeşil rengi ile dolmuş olmasına dikkat edin.

**3. Adım.** *Temel Parolayı Onaylayın* ekranını etkinleştirmek için 'ı **tıklayın** ve parolanızı aşağıda görüldüğü gibi teyit edin:



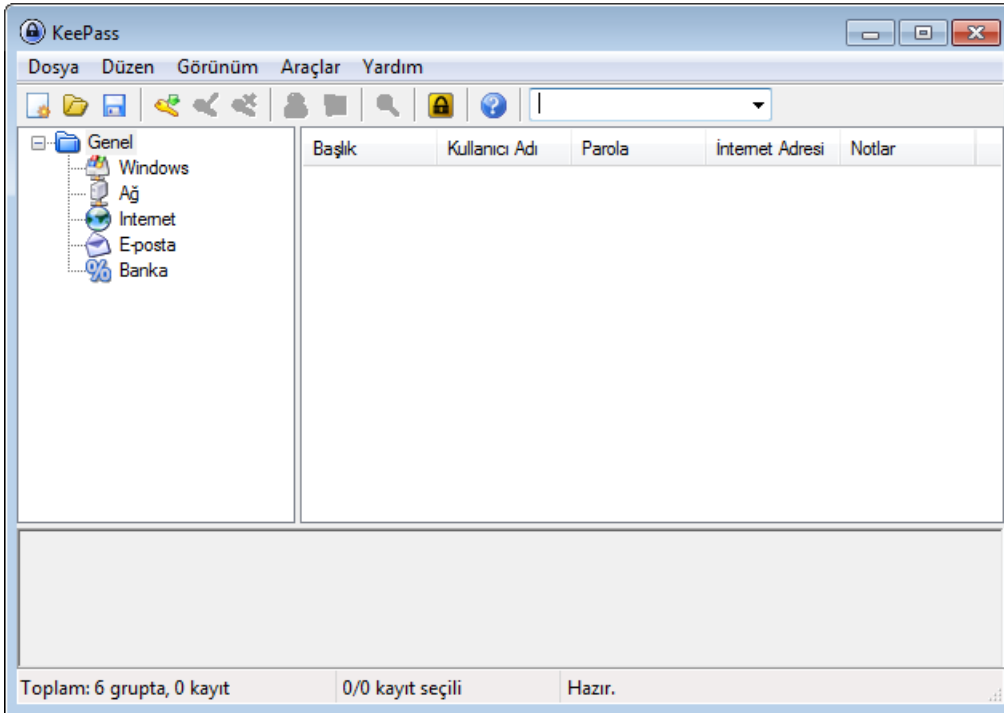
Şekil 11: KeePass Temel Parolayı Onaylayın ekranı

**4. Adım.** Daha önce girmiş olduğunuz Parolayı **tekrarlayın** ve 'ı **tıklayın**.

**5. Adım.** Parolanızı doğru girdiğinizden emin olmak için 'e **tıklayın**.

**Uyarı:** Etrafınızda girdiğiniz Parolayı görecektir birileri varsa 5. Adım'ı uygulamayın.

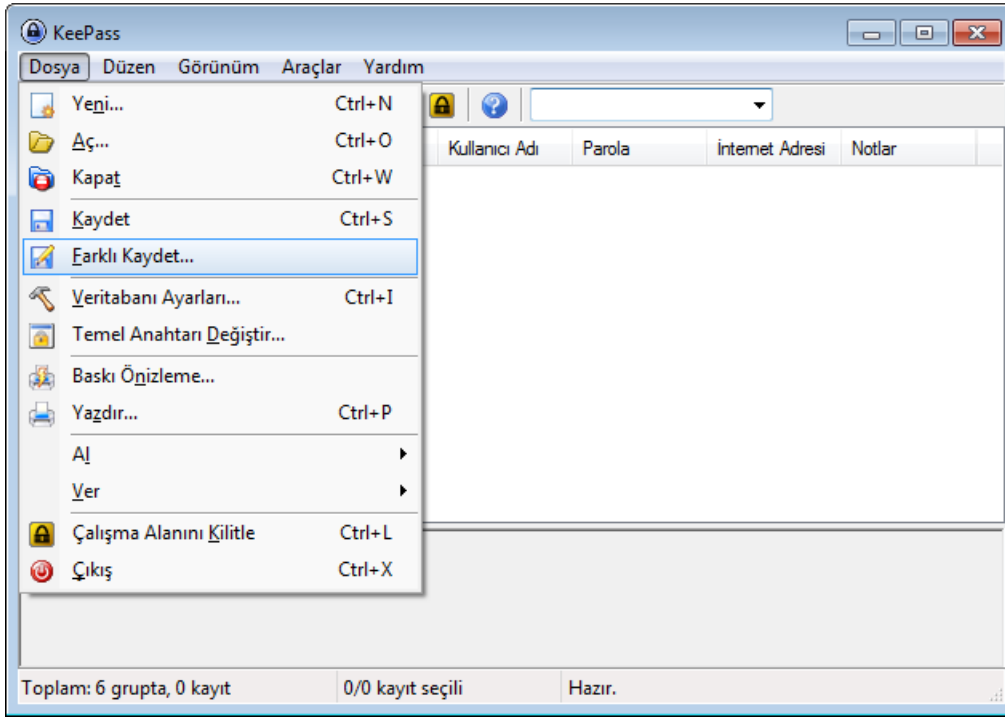
Temel parolanızı başarılı bir şekilde iki defa girdikten sonra **KeePass** konsolu aşağıda görüldüğü gibi etkinleşecektir:



Şekil 12: Etkinleşmiş KeePass Parola Güvenliği ekranı

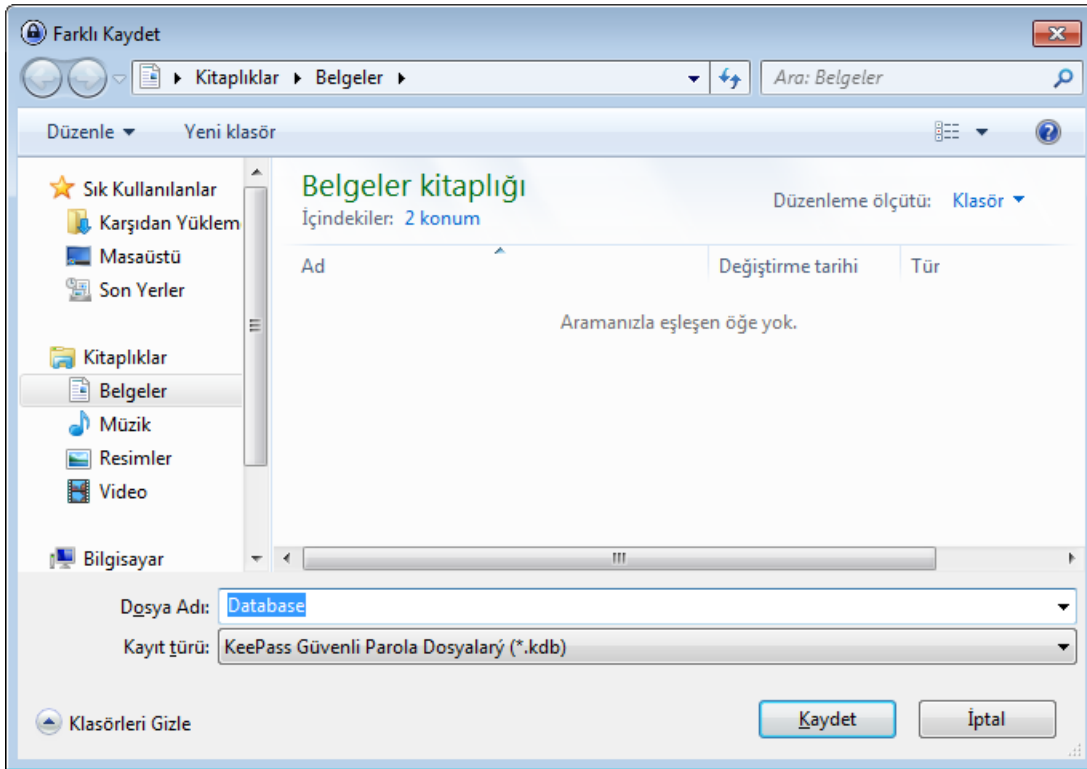
Parola veri tabanınızı oluşturduktan sonra onu kaydetmeniz gerekir. Parola veri tabanını kaydetmek için aşağıdaki adımları takip ediniz:

**1. Adım.** **Dosya > Farklı Kaydet**'i aşağıdaki gibi seçin:



Şekil 13: KeePass Parola Güvenliği ekranı

Bu, Farklı Kaydet ekranını aşağıda görüldüğü gibi etkinleştirecek:



Şekil 14: Farklı Kaydet ekranı

**2. Adım.** Yeni Parola veri tabanınız için bir isim **girin**.

**3. Adım.** Veri tabanınızı kaydetmek için **Kaydet** butonuna tıklayın.

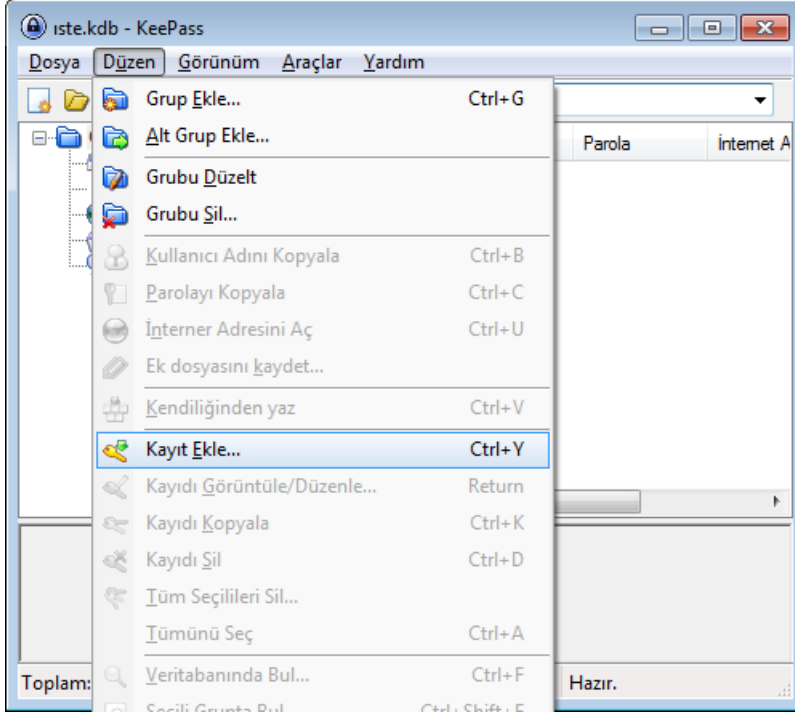
**İpucu:** Veri tabanınızın yerini ve dosya ismini unutmayın! Veri tabanını yedeklemek istediğiniz zaman bu bilgiler işinizi kolaylaştıracaktır.

Tebrikler! Güvenli Parola veri tabanınızı başarılı bir şekilde oluşturduunuz ve kaydettiniz. Şimdi bu veri tabanını var olan ve yeni oluşturacağınız Parolalarla doldurabilirsiniz.

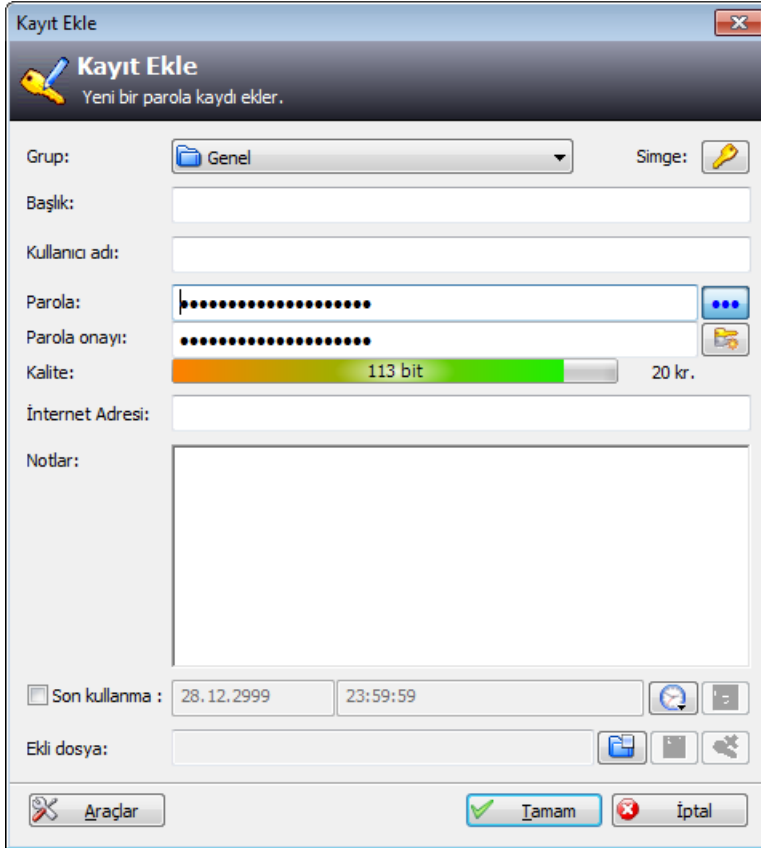
## 2.3. Nasıl Kayıt Eklenir

Kayıt Ekle ekranı, yeni oluşturduğunuz veri tabanına hesap bilgilerinizi, Parola ve diğer önemli bilgilerinizi girmenize olanak sağlar. Aşağıda görünen örnekte olduğu gibi, farklı web siteleri ve e-posta hesapları için Parola ve kullanıcı adı girişi yapabilirsiniz.

**1. Adım.** Kayıt Ekle ekranını etkinleştirmek için aşağıda görüldüğü gibi **KeePass Parola Güvenliği** ekranında **Düzenle – Kayıt Ekle**'yi seçin:



Şekil 15: Düzenle > Kayıt Ekle seçili KeePass Parola Güvenliği ekranı



Şekil 16: KeePass Kayıt Ekle ekranı

**Not:** Kayıt Ekle ekranında doldurmanız gereken birçok alan vardır. Bu alanları doldurmak zorunlu değildir, eklediğiniz bilgiler daha çok size kolay sağlaması için eklenir. Belli bir girişi aradığınız durumlarda işinize yarayabilir.

Aşağıda bu kutular ile ilgili kısa açıklamaları bulabilirsiniz:

- **Grup:** KeePass Parolalarınızı önceden belirlediğiniz grupların içine yerleştirmenize olanak sağlar. Örneğin, web

sitesi hesaplarınızın Parolalarını 'İnternet' grubu adı altında toplayabilirsiniz.

- **Başlık:** Belli bir Parola girişini tanımlamak için ona bir isim verebilirsiniz. Örneğin: Gmail Parolası
- **Kullanıcı Adı:** Parola girişi ile bağlantılı kullanıcı adı. Örneğin: securitybox@gmail.com.
- **URL:** Parola girişi ile bağlantılı internet sitesi. Örneğin: https://mail.google.com.
- **Parola:** Bu özellik, *Kayıt Ekle* ekranı etkinleştirildiği zaman otomatik olarak rastgele bir Parola oluşturur. Yeni bir e-posta hesabı açıyorsanız, bu alanda görünen 'verili' Parolayı kullanabilirsiniz. Bu özelliği, var olan bir Parolayı **KeePass'in** oluşturduğu bir Parola ile değiştirmek için de kullanabilirsiniz. **KeePass** Parolaları sizin için hatırlayacağından, bu Parolayı görmenize gerek yoktur. Rastgele oluşturulmuş bir Parola her zaman kuvvetlidir (tahmin edilmesi veya kırılması kolay değildir).

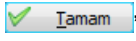
Aşağıdaki bölümde rastgele bir Parolanın nasıl oluşturulacağı anlatılır. Elbette, verili Parolayı istediğiniz başka bir Parola ile değiştirebilirsiniz. Örneğin, var olan bir hesabınızın girişini yapıyorsanız oraya kullandığınız Parolayı girmek isteyebilirsiniz.

- **Parola Onayı:** Parolanın teyit edilmesi.
- **Kalite:** Parolanın uzunluk ve rastlantısallığa göre ölçülen gücünü gösteren ilerleme çubuğu. Bu çubuk üzerindeki yeşil rengi ne kadar artarsa, Parolanız o kadar güçlü demektir.
- **Notlar:** Bilgi sakladığınız hesap veya site ile ilgili genel bilgileri ve tanımları girdiğiniz yer. Örneğin: *Mail sunucu ayarları: POP3 SSL, pop.gmail.com, Port 995; SMTP TLS, smtp.gmail.com, Port: 465.*

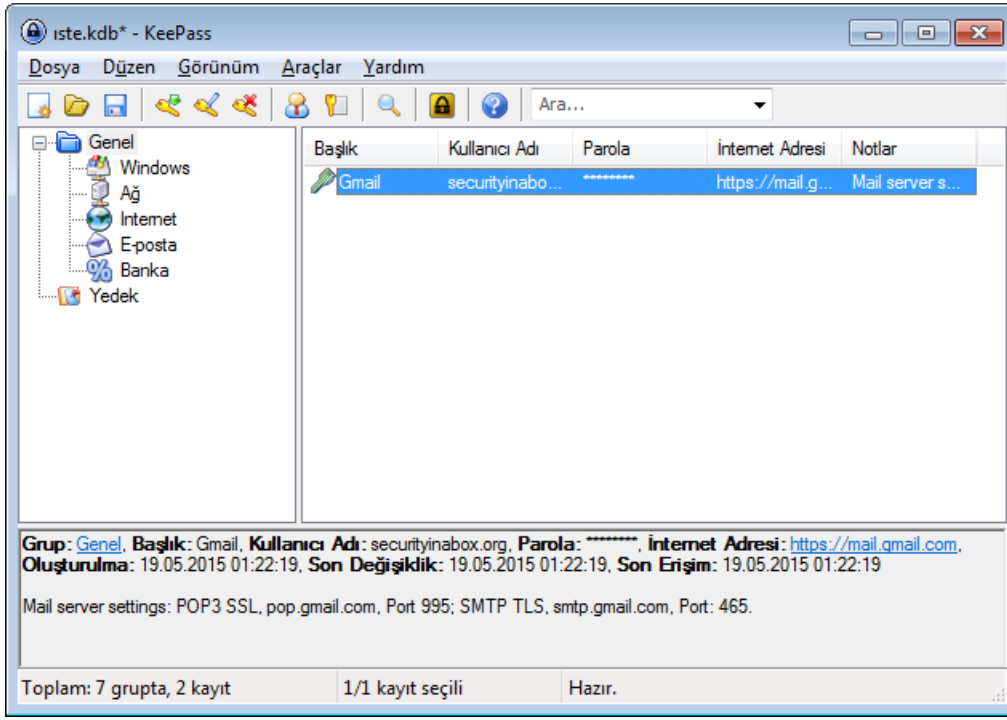
**Not: KeePass'te** Parola kayıtları oluşturmak veya onları modifiye etmek gerçek Parolalarınızı değiştirmez! **KeePass'i** Parolalarınızı akladığınız güvenli, elektronik bir adres defteri olarak düşünebilirsiniz. Sadece sizin oraya yazdıklarınızı saklar, başka bir işlevi yoktur.

Aşağı-açılır menüden *İnternet'i* seçerseniz, Parola kaydınız aşağıdaki gibi görünür:

Şekil 17: KeePass Kayıt Ekle ekranı – tamamlanmış

**2. Adım.** Giriş Yap ekranında yaptığınız değişiklikleri kaydetmek için 'ı tıklayın.

Parola kaydınız şimdi *İnternet Grubunda* görünecektir.



Şekil 18: KeePass Parola Güvenliği ekranı

**Not:** Bu pencerenin alt kısmı seçili olan giriş hakkında bilgi verir. Bu bilgiler arasında girişin oluşturulma, düzenlenme ve son kullanma tarihleri ve girmiş olduğunuz diğer notlar vardır. Parola, gösterilen bu bilgilere dahil değildir.

- **Son Erişim:** Son erişim tarihi belirleyebileceğiniz metin kutularını etkinleştirmek için bu özelliğe bakınız. Bu şekilde, Parolanızı belli tarihlerde (örneğin her 3 ayda bir) değiştirmek için kendinize hatırlatma yapabilirsiniz. Bir Parolanın kullanım süresi bittiği zaman, isminin yanında aşağıda görüldüğü gibi kırmızı bir çarpı işareti çıkacaktır:

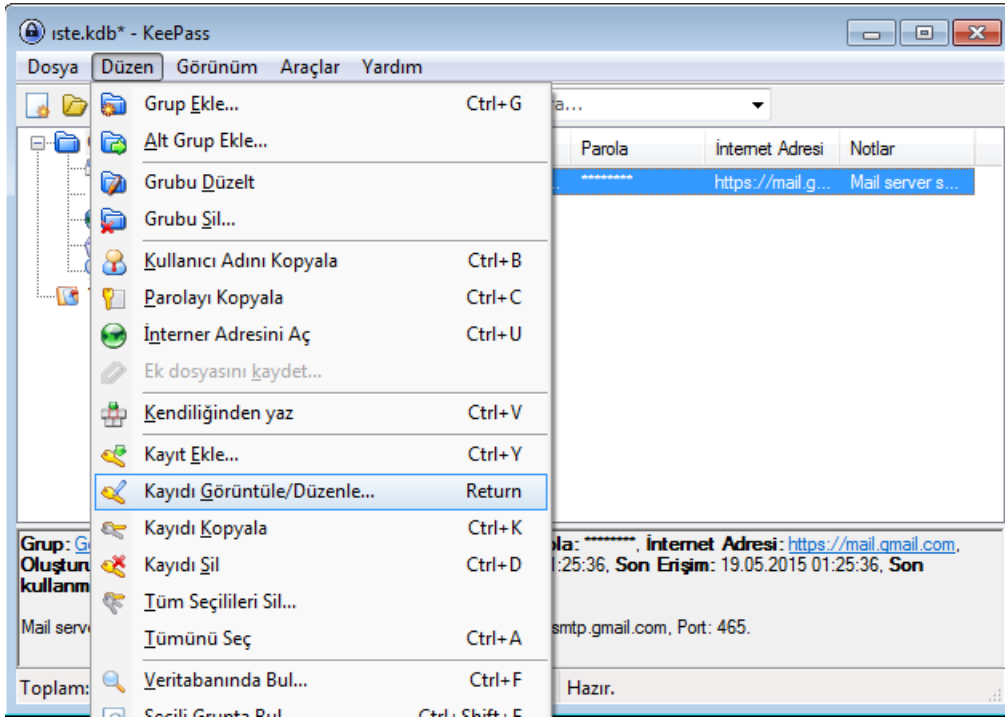
Şekil 19: NetSecureDb.kdb ekranında süresi dolmuş bir parola örneği

## 2.4 Bir Kayıt Nasıl Düzenlenir

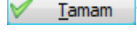
**KeePass'e** yaptığınız herhangi bir kaydı istediğiniz zaman düzenleyebilirsiniz. Parola kaydınızdaki parolayı değiştirebilir veya diğer bilgileri düzenleyebilirsiniz. Her üç veya altı ayda bir Parolanızı değiştirmeniz önerilir (Parolayı KeePass'te değiştirmeden önce e-posta sisteminizde güncellemeyi unutmayın).

Bir girişi düzenlemek için aşağıdaki adımları takip edin:

- 1. Adım.** İlgili kayıtları etkinleştirmek için, sol taraftaki *Grup'lardan* gerekli olanını **seçin**.
- 2. Adım.** İlgili kaydı **seçin** ve aşağıda görünen pencereyi etkinleştirmek için taraftan seçili olan girişin üzerine **sağ tıklayın**.



Şekil 20: Düzenle menüsünü gösteren KeePass Parola Güvenliği ekranı

**3. Adım.** Parola ve bilgilerde yapmış olduğunuz değişiklikleri kaydetmek için 'ı tıklayın.

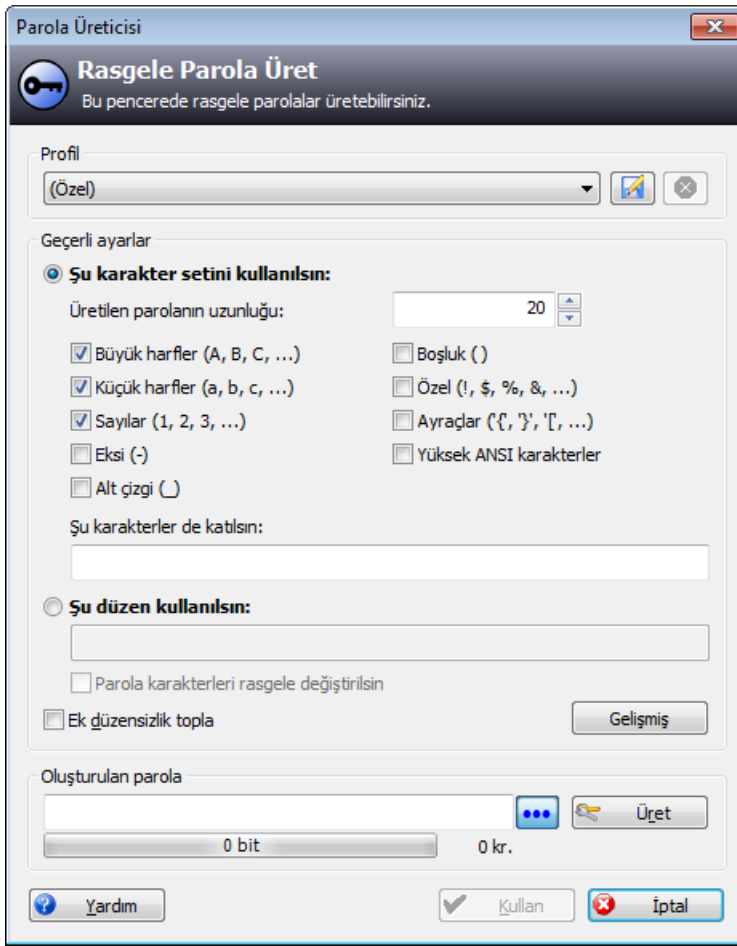
Daha önce kendi oluşturduğunuz bir Parolayı **KeePass'ın** oluşturduğu ve önerdiği bir Parola ile değiştirmek için aşağıdaki bölümü okuyunuz.

## 2.5 Rastgele Parolalar Nasıl Üretilir

Uzun ve rastgele Parolalar güvenlik dünyasında güçlü kabul edilir. Bu rastlantısalılık çeşitli matematik prensiplerine göre oluşturulur ve hesaplarınızdan birine girmeye çalışan bir kişi tarafından basitçe 'tahmin edilemez'. Böyle bir Parola oluşturmanız için **KeePass** size bir *Parola Üretici* sunar. Yukarıda gördüğünüz gibi, yeni bir giriş yaptığınız zaman otomatik olarak rastgele bir parola oluşturulur. Bu bölümde, böyle bir parolayı kendiniz oluşturmak isterseniz bunu nasıl yapacağınız anlatılır.

**Not:** *Parola Üretici*, *Kayıt Ekle* ve *Düzenle/Kayıt Görüntüle* ekranlarından etkinleştirilebilir. Ya da, **Araçlar – Parola Üretici seçerek** açılabilir.

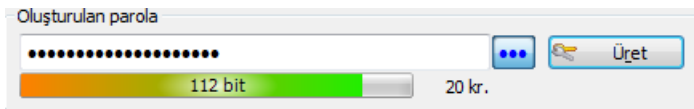
**1. Adım.** *Kayıt Ekle* ya da *Düzenle/Kayıt Görüntüle* ekranından 'i tıklayın. **Parola Üretici** ekranı aşağıda görüldüğü gibi etkinleşecektir:



Şekil 21: KeePass Parola Üretici ekranı

Parola Üretici ekranı, Parola oluşturmak için çeşitli seçenekler sunar. Parolanızın uzunluğunu, içinde yer alacak karakterleri ve diğer bilgileri buradan seçebilirsiniz. Şu anki amacımız doğrultusunda verili seçenekleri kullanabiliriz. Bu Parolanın 20 karakterden ve küçük ve büyük harflerden oluşacak anlamına gelir.

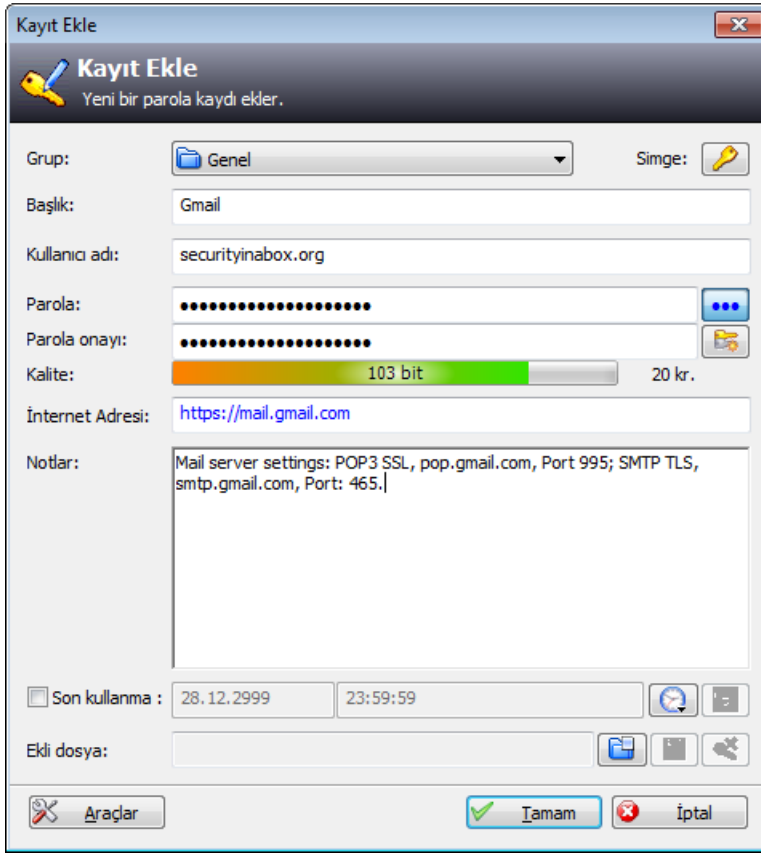
**2. Adım.** İşleme başlamak için (Oluştur)'i **tıklayın**. İşlem bittiği zaman **KeePass** sizin için bir parola üretmiş olacaktır.



Şekil 22: KeePass Oluşturulan Parola ekranı

**Not:** Üretilen parolayı  e basarak görebilirsiniz. Fakat, yukarıda da bahsettiğimiz gibi bu bir güvenlik riski oluşturabilir. Aslında, oluşturulan bu Parolayı görmeniz gerekmez. Bu durumla ilgili **3.0 KeePass Parolalarını Kullanma** <sup>[10]</sup> kısmında daha çok bilgi vereceğiz.

**3. Adım.** Parolayı kabul etmek için  **Kullan** 'ı **tıklayın** ve aşağıda görünen *Kayıt Ekle* ekranına geri dönün:



Şekil 23: KeePass Giriş Kayıt Ekle ekranı

**4. Adım.** Bu kaydı kaydetmek için (Kaydet)'i **tıklayın**.

**5. Adım.** Güncellenmiş parola veri tabanınızı kaydetmek için **Dosya > Kaydet**'i seçin.

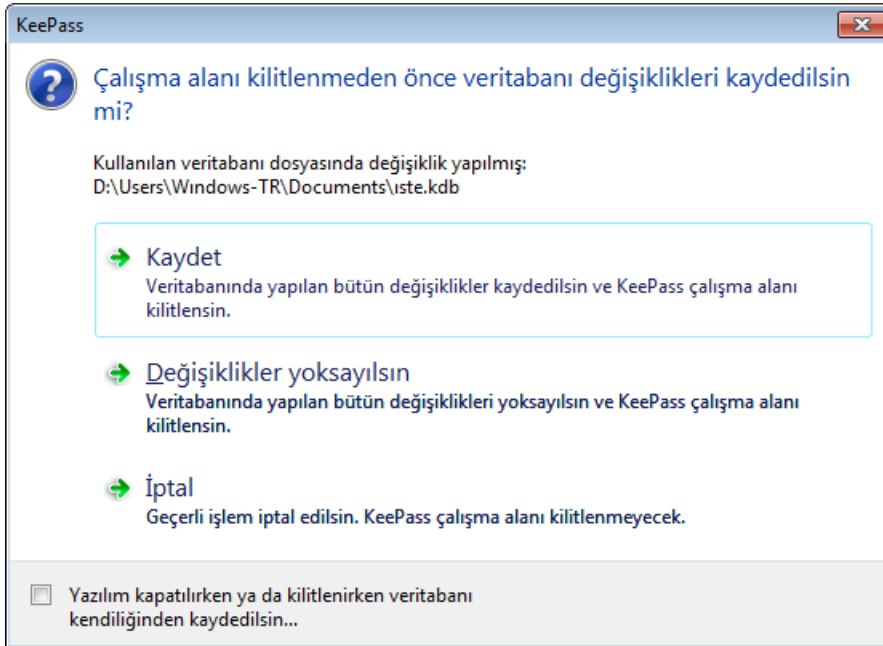
## 2.6 KeePass Nasıl Küçültülür, KeePass'ten Nasıl Çıkılır

**KeePass** programını istediğinizde simge durumuna küçültebilir veya kapatabilirsiniz. Tekrar açtığınız veya eski durumuna getirdiğinizde, *Temel Parolanızı* girmeniz istenecek.

**KeePass** bildirim alanınızda şu şekilde görünecek şekilde kendini simge durumuna getirir:

**KeePass** programını aşağıdaki adımları takip ederek de kilitleyebilirsiniz:

**1. Adım.** Aşağıdaki ekranı etkinleştirmek için **Dosya > Çalışma Alanını Kilitle**'yi Seçin:

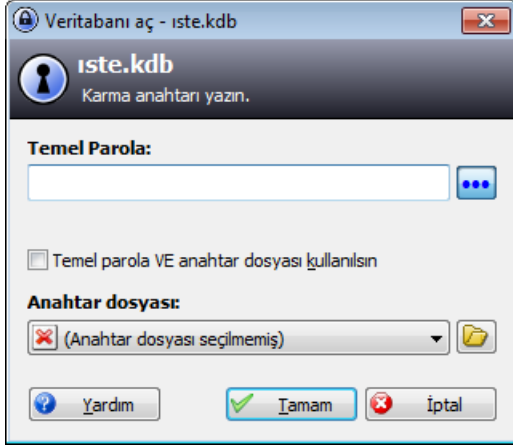


Şekil 24: KeePass – Kapatmadan/Kilitlemeden Önce Kaydet komut ekranı

**2. Adım.** Bilgileriniz kaydetmek ve **KeePass** konsolunu *Şekil 3'te* görüldüğü gibi etkin olmaktan çıkarmak için [Kaydet](#) i **tıklayın**. Bildirim alanınızda şu ikon görünecektir: .

**KeePass'i** eski durumuna getirmek için aşağıdakini yapınız:

**1. Adım. KeePass'i** eski boyutuna getirmek için ve aşağıdaki ekranı etkinleştirmek için ikonun üzerine **çift tıklayın**.



*Şekil 25: KeePass Veri Tabanını Aç – NetSecureDb.kdb ekranı*

**2. Adım. KeePass'i** açmak için **Temel Parolanızı girin**.

**KeePass'i** kapatmak için aşağıdaki adımı uygulayın:

**1. Adım. KeePass** programını tamamen kapatmak için **Dosya > Çıkış'ı seçin**.

Veri tabanında kaydedilmemiş değişiklikleriniz varsa **KeePass** bunları kaydetmenizi isteyecektir.

## 2.7 Parola Veritabanı Dosyası Nasıl Yedeklenir

Bilgisayarınızdaki **KeePass** veri tabanı dosyaları .kdb uzantısından tanınabilir. Bu dosyayı bir USB hafıza çubuğuna aktarabilirsiniz. Temel Parola olmadan bu veri tabanını kimse açamaz.

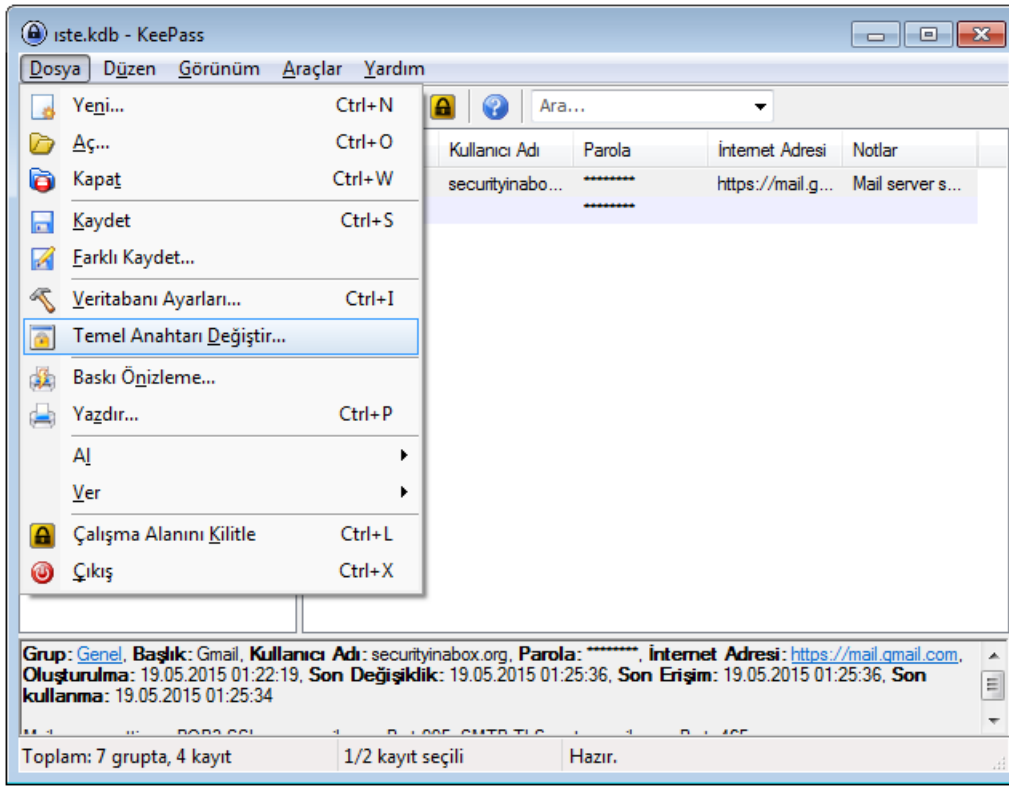
**1. Adım.** Ana ekrandan **Dosya– Farklı Kaydet'i seçin** ve veri tabanını başka bir yere kaydedin.

Tüm KeePass programını bir USB hafıza çubuğundan çalıştırabilirsiniz. Bunun için lütfen [Taşınabilir KeePass](#) <sup>[11]</sup> bölümüne bakın.

## 2.8 Temel Anahtar Nasıl Yeniden Tanımlanır

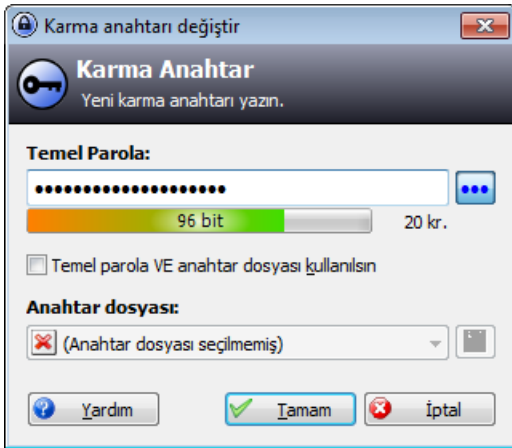
**Temel Anahtarınız** istediğiniz zaman değiştirebilirsiniz. Bunu Parola veri tabanını açtıktan sonra yapabilirsiniz.

**1. Adım. Dosya > Temel Anahtarı Değiştir'i Seçin**



Şekil 26: KeePass Temel Anahtar'ı Değiştir ekranı

2. Adım. Sorulduğunda Temel Anahtarınızı girin.



Şekil 27: KeePass Temel Anahtar Değiştir ekranı

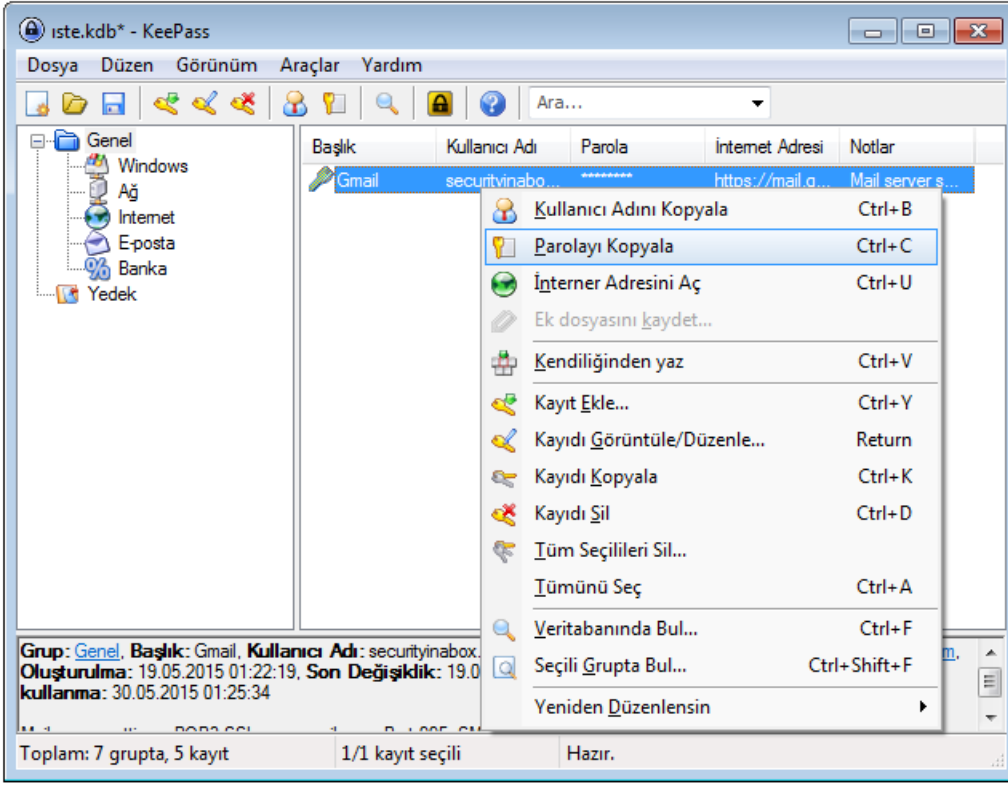
## Keepass Parolaları Nasıl Kullanılır

### 3.0 Keepass Parolaları Nasıl Kullanılır

Güvenli bir parola kolay akılda tutulamaz iken, KeePass parolayı veri tabanından kopyalayıp herhangi bir hesap veya web sitesine yapıştırmanıza izin verir. Daha yüksek bir güvenlik için, kopyalanmış olan parola, taşıma panosunda sadece 10 saniye kalır, bu yüzden hesabınızı veya web sitesini önceden açmak ve parolayı daha sonra kopyalayıp yapıştırmak zaman size kazandırır.

1. Adım. Aşağı-açılır menüyü etkinleştirmek için ilgili parolaya **sağ tıklayın**.

2. Adım. **Parolayı Kopyala'yı** aşağıda görüldüğü gibi **seçin**:



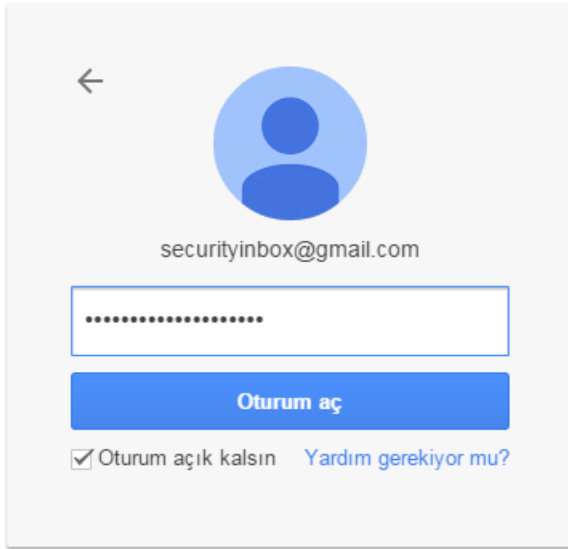
Şekil 1: KeePass Parola Güvenliği ekranı

3. Adım. İlgili hesap veya siteye gidin ve parolayı gereken yere **yapıştırın**:



# Tek hesap. Tüm Google.

Devam etmek için Gmail'de oturum açın



Şekil 2: Yapıştırılmış parolayı gösteren Gmail Hesabı

**İpucu:** Daha verimli bir şekilde kopyalamak, yapıştırmak ve pencere değiştirmek için kısa yolları kullanın. Parolayı kopyalamak için **Ctrl** tuşunu **basılı tutarak C** tuşuna basın. Parolayı yapıştırmak için **Ctrl** tuşuna **basılı tutarak V** tuşuna basın. Açık olan program ve pencereler arasında geçiş yapmak için **Alt** tuşuna **basılı tutarak Tab** tuşuna basın.

**Not:** Sürekli **KeePass** kullanırsanız parolanızı bilmenize ve görmenize gerek kalmaz. Kopyala/Yapıştır fonksiyonları parolayı veri tabanından gereken pencereye taşımaya olanak sağlar. Rastgele Parola Oluşturma özelliğini kullanıyorsanız ve sonra bu parolayı yeni bir e-posta hesabı oluşturma işlemine taşıyorsanız, hiçbir zaman görmek zorunda olmadığınız bir parola kullanabilirsiniz. Ve bu parola etkin bir şekilde çalışır!

# Taşınabilir KeePass

## Short Description:



**Portable KeePass** is a secure and easy-to-use password management tool.

List of sections on this page:

- [4.1 Kurulu ve Taşınabilir KeePass Sürümleri Arasındaki Farklar](#)
- [4.2 Taşınabilir KeePass Nasıl İndirilir ve Paketinden Çıkartılır](#)

## 4.1 Kurulu ve Taşınabilir KeePass Sürümleri Arasındaki Farklar

Taşınabilir araçlar yerel bir bilgisayara kurulu olmadıkları için, varlık ve kullanımları kolayca saptanamaz. Fakat unutmayın ki, taşınabilir araçlarınız ve USB hafıza çubuklarınız, ancak kullandığınız bilgisayar kadar güvenlidir ve reklam destekli bilgisayar yazılımlar, casus yazılımlar veya kötü amaçlı yazılımlara maruz kalabilir.

Taşınabilir **KeePass** ve kurulu sürüm arasında bunun dışında hiçbir fark yoktur.

## 4.2 Taşınabilir KeePass Nasıl İndirilir ve Paketinden Çıkartılır

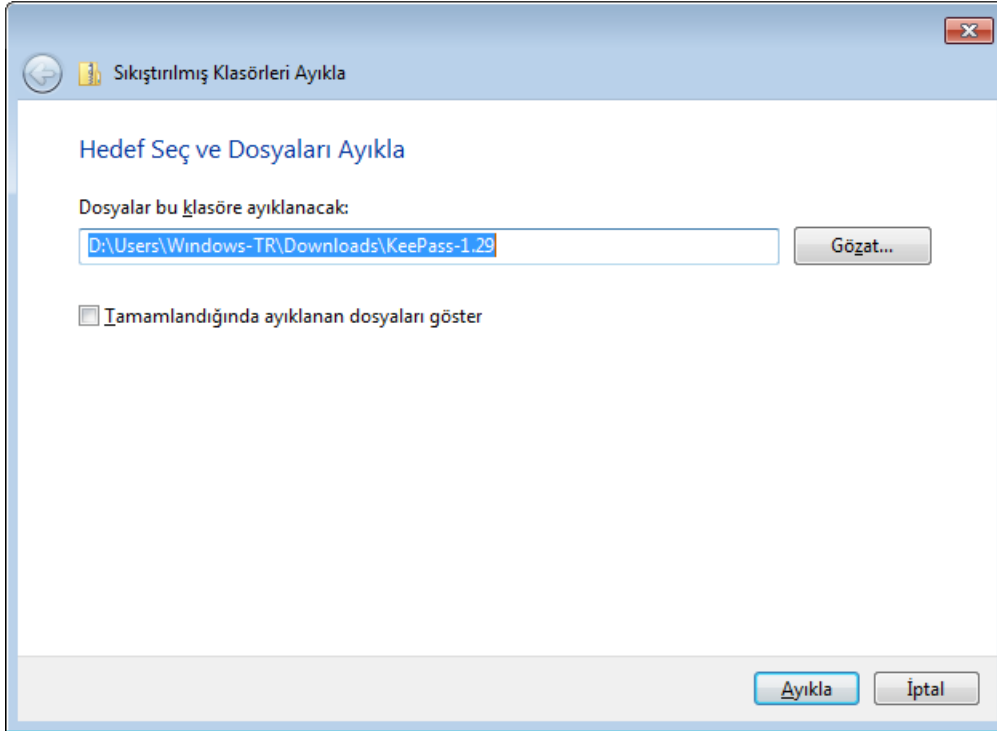
1. Adım. <http://keepass.info/download.html>'a <sup>[12]</sup> **tıklayın**, ilgili indirme sitesine yönlendirileceksiniz.



2. Adım. **Source Forge** indirme sayfasını etkinleştirmek için **tıklayın**.

3. Adım. Kurulum dosyasını bilgisayarınıza kaydetmek için **KeePass-1.29** **tıklayın** ve kaydettiğiniz dosyayı **açın**.

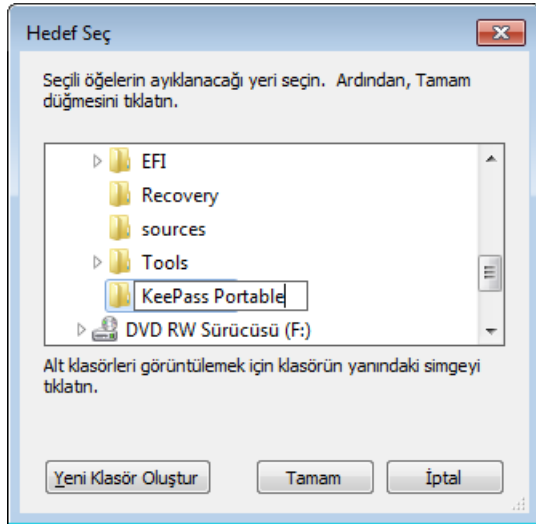
4. Adım. Aşağı-Açılır menüyü etkinleştirmek için **KeePass-1.29** **sağ tıklayın** ve **Tümünü Ayıkla'yı seçin**. Aşağıdaki ekran etkinleşecektir:



Şekil 1: Bir Hedef seçin ve Dosyaları Ayıklayın

5. Adım. **Gözet'i tıklayarak** aşağıda **Şekil 2'de** görüldüğü gibi, çıkarılabilir sürücünüze veya USB hafıza çubuğunuza gidin ve **Yeni Klasör Oluştur** **tıklayın**.

6. Adım. Yeni dosyanız için, E:\ 'de veya aşağıdaki Şekil 2'te gösterilen dosya ağacında bir isim **girin** ve **Tamam'ı tıklayın**.

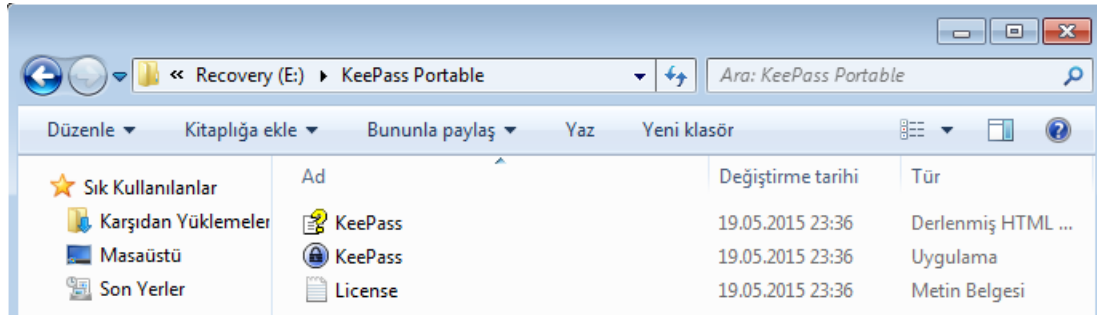


Şekil 2: Çıkarma yolu ve pencere dosya ağacı seçenekleri (boyutu değiştirilmiş)

**Not: Taşınabilir KeePass** dosyası için değişik bir isim oluşturmak onun varlığını ve kullanımını daha zor tespit edilebilir hale getirebilir.

7. Adım. **Taşınabilir KeePass'i** Paketinden çıkarmak ve yeni oluşturulan **Taşınabilir KeePass** dosyasına aktarmak için **Ayıkla** 'yı tıklayın.

8. Adım. Çıkarılabilir sürücünüze veya USB hafıza çubuğunuza **gidin** ve **Taşınabilir KeePass** dosyasını **açın**.



Şekil 3: Yeni çıkarılmış Taşınabilir KeePass dosyasını gösteren, çıkarılabilir sürücü penceresi

9. Adım. **Taşınabilir KeePass'i** kullanmaya başlamak için **KeePassPortable.exe**'ye **çift tıklayın**.

**KeePass'i** nasıl kullanacağınıza dair yönergeler için ile ilgili olarak lütfen yukarıdaki **KeePass** [13] bölümüne başvurunuz.

#### Offline Installation Instructions :

##### KeePass'i İndirme

- Kısa **Uygulamalı Rehberler'in** [1] Giriş bölümünü okuyun
- Aşağıdaki **Keepass** ikonunu **tıklayıp** kurucuyu 'Açın' ya da 'Çalıştırın'. Gerekirse kurucuyu ilk önce kaydedin ve sonrasında bulup üzerine çift tıklayın
- Devam etmeden önce bir sonraki kısımdaki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz, kurulumdan sonra silebilirsiniz

KeePass:



[14]

## Sıkça Sorulan Sorular ve Gözden Geçirme

### 5.0 Sıkça Sorulan Sorular ve Gözden Geçirme

**KeePass** kullanımı oldukça kolay bir programdır. Önemli olan **KeePass'te** yeni parola oluşturma alışkanlığı kazanabilmektir. Parolalarınızı bilmiyormak size zor gelebilir, fakat emin olun ki bu onları hatırlamaktan daha kolaydır!

**Soru:** Ana şifremi unutmam durumunda, **KeePass'e** erişmem ve şifre veri tabanına ulaşmam mümkün müdür?

**Cevap:** Hayır. Bu durumda yapabileceğiniz hiçbir şey yoktur. Fakat, işin iyi tarafı, başka kimsenin de şifrelerinize ulaşamayacak olmasıdır! Bunun olmasını engellemek için, Nasıl Yapmalı Kitapçığı'nın 3. Bölümü **Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** [4] bölümüne bakabilir ve burada önerilen parola hatırlama metodlarından faydalanabilirsiniz.

**Soru:** KeePass programını kaldırırsam şifrelerime ne olur?

**Cevap:** Program bilgisayarınızdan silinmiş olur, fakat, veri tabanınız (.kdb dosyasında kaydedilmiş olan) silinmeyecektir. KeePass programını yeniden kurduğunuz zaman bu dosyaya anında ulaşabilirsiniz.

**Soru:** Sanırım veri tabanı dosyasını yanlışlıkla sildim!

**Cevap:** Umarız daha önceden bir yedekleme yapmışsınızdır. Bunun yanı sıra, dosyayı ilk başta nereye kaydettiğinizi unutmadığınızdan emin olun. Bilgisayarınızda .kdb uzantılı bir dosya aratın. Gerçekten silmiş iseniz, **Recuva** [15] kılavuzuna bakın. Bu kılavuz dosyanızı geri kazanmanıza yardımcı olabilir.

## 5.1 Gözden Geçirme Soruları

- Bir parolayı güçlü yapan nedir?
- KeePass'teki bir parola kaydını nasıl gözden geçirebilirsiniz?
- KeePass'te nasıl otuz karakterli bir parola oluşturabilirsiniz?

# TrueCrypt – Güvenli Dosya Muhafazası

### Short Description:

**\*\*Truecrypt\*\***, dosyalarınıza doğru şifreye sahip olmayan kimselerin ulaşmasını engelleyerek onları güvenli bir şekilde depolamanızı sağlar. Dosyalarınızı güvenli bir şekilde saklayabileceğiniz elektronik bir kasa gibidir.

### Online Installation Instructions:

TrueCrypt'i indirme - TrueCrypt programının geliştirmesi konusundaki belirsiz durum ve geliştiricilerin web sitesinde sundukları son sürüm hakkındaki bilgi eksiklikleri (aşağıdaki açıklamaya bakınız) yüzünden, burada kurulum programlarından arşivlenmiş olan 7.1a sürümünü sunuyoruz.

- İşletim sisteminizin kurulum programını indirmesi için aşağıdaki bağlantıya **tıklayın**.
- Kurucuyu bilgisayarınıza kaydedin, kaydettiğiniz yere **gidin** ve üzerine **çift tıklayın**.
- **TrueCrypt'i** başarılı bir şekilde kurduktan sonra, kurulum programını bilgisayarınızdan silebilirsiniz.

### TrueCrypt:



- **MS Windows sürümü** [16] (**doğrulama imzası** [17])
- **Mac OS X sürümü** [18] (**doğrulama imzası** [19])
- **Linux 32 bit sürümü** [20] (**doğrulama imzası** [21])
- **Linux 64 bit sürümü** [22] (**doğrulama imzası** [23])
- **Linux konsolu 32 bit sürümü** [24] (**doğrulama imzası** [25])
- **Linux konsolu 64 bit sürümü** [26] (**doğrulama imzası** [27])
- **Kaynak Kodu** [28] (**doğrulama imzası** [29])
- **Sürüm Geçmişi** [30]
- TrueCrypt Kuruluşu açık GPG anahtarı: [keys.mozilla.org](https://keys.mozilla.org) kopyası [31] (**yerel kopya** [32]). **Tor projesinden yazılım imzaları nasıl doğrulanır?** [33]. bölümündeki talimatlara bakın.
- Ayrıca bakınız: <https://truecrypt.ch/downloads/> [34]

28 Mayıs 2014 tarihinde TrueCrypt geliştirici web sitesi, kullanıcılarına TrueCrypt gelişiminin şimdilik durduğunu haber verdi. Bu durumun arkasında yatan nedenler hala belli değil. Geliştirici web sitesi, TrueCrypt'in daha yeni ama bazı işlevleri kaldırılmış 7.2 sürümünü sunuyor. Bu yeni sürümün varlığına rağmen, gelişiminin durdurulmasının arkasındaki nedenleri ve TrueCrypt gelişimi ile ilgili gelecekte bizleri neler beklediğini öğrenene kadar, eski sürüm 7.1a'yı kullanmanızı öneririz (Kurulum Talimatlarına bakınız). TrueCrypt'e alternatif programlar

için aşağıdaki “GNU Linux, Mac OS ve diğer Microsoft Windows ile Uyumlu Programlar” bölümüne bakınız.

Ana Sayfa

[www.truecrypt.org](http://www.truecrypt.org)

## Bilgisayar Gereksinimleri

- Windows 2000/XP/2003/Vista/7
- Var olan birimlere erişmek için değil ama programın kurulumu ve yeni birim yaratmak için yönetici hakları gerekmektedir.

## VBu kılavuzda kullanılan sürüm

- 7.1a

## Bu bölümün son güncellenme tarihi

- Mayıs 2014

## Lisans

- Özgür ve Açık Kaynak Yazılım

## Taşınabilir Sürüm

- [Taşınabilir TrueCrypt için Uygulamalı Rehberler](#) <sup>[35]</sup>

## Gerekli Okumalar

- Nasıl Yapmalı Kitapçığı [4. Bilgisayarınızdaki hassas dosyaları nasıl korursunuz](#) <sup>[36]</sup> bölümü

## Buradan sağlayacağınız faydalar:

- Dosyalarınızı kötü amaçlı kimselerden ve izinsiz erişimlerden etkin bir şekilde koruyabilmek
- Önemli dosyalarınızın kopyalarını kolay ve güvenli bir şekilde muhafaza edebilmek

## GNU Linux, Mac OS ve Microsoft Windows ile Uyumlu Diğer Programlar:

**Not: TrueCrypt, GNU Linux ve Mac OS için de uygundur.**

**Ubuntu** <sup>[37]</sup> gibi birçok **GNU Linux** dağıtımı, standart bir özellik olarak, tüm sürücü için anında oluşturulan şifreleme ve şifre çözme özelliklerini destekler. Sistemi kurduğunuz zaman bu özelliği kullanıp kullanmayacağınıza karar verebilirsiniz. Ayrıca, kurulum esnasında ana klasör için şifreleme özelliğini açmanızı öneririz. **Linux** sisteminize , **dm-crypt** <sup>[38]</sup> ve **cryptsetup and LUKS** <sup>[39]</sup> kullanarak da şifreleme özelliği ekleyebilirsiniz. Bir başka olasılık da, özgür ve açık yazılım olan ve anında şifreleme-şifre çözme özelliğini kullanan **SD4L (ScramDisk için Linux)** <sup>[40]</sup> programını kullanmaktır.

**Mac OS** için **FileVault** kullanabilirsiniz. Bu işletim sisteminin bir parçasıdır ve tüm sürücünüz ve/veya ana klasörünüz ve alt klasörleriniz için *anında* şifreleme ve şifre çözme özelliği vardır.

**Microsoft Windows** için alternatif olarak şunları öneririz:

- **DiskCryptor** <sup>[41]</sup> sistem bölmesi dahil tüm sürücü bölmeleriniz için şifreleme sağlayan özgür, açık kaynak şifreleme programıdır.
- **AxCrypt** <sup>[42]</sup> farklı dosyaları şifreleyebilen özgür ve açık kaynak bir programdır.

MS Windows 7 Ultimate veya Enterprise sürümlerine veya MS Windows 8 Pro ve Enterprise sürümlerinde, tüm sürücünüzü şifrelemek için **BitLocker**'i <sup>[43]</sup> bulabilirsiniz. Fakat unutmayın ki, BitLocker, bilgilerinizi koruma ve güvenlik sağlama amacını nasıl yerine getirdiği bağımsız olarak denetlenmemiş, kapalı ve tescilli bir Microsoft ürünüdür.

## 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

**TrueCrypt** verilerinizi sizin oluşturacağınız bir şifre ile korumaya yardımcı olur. Bu şifreyi unutursanız, verilerinize erişiminizi kaybedersiniz! **TrueCrypt**, dosyalarınızı korumak için şifreleme denen bir işlem kullanır. Lütfen aklınızda tutun ki bazı ülkelerde şifreleme yasal değildir. **TrueCrypt**, belli başlı dosyaları şifrelemek yerine, bilgisayarınızda birim denilen, korunmuş bir alan yaratır. Bu şifrelenmiş birim içerisinde dosyalarınızı güvenli bir şekilde muhafaza edebilirsiniz.

**TrueCrypt**, şifrelenmiş bir standart birim veya bir gizli birim oluşturmanıza olanak verir. İkisi de dosyalarınızı gizli tutacaktır, fakat gizli birim, önemli bilgilerinizi daha az hassas olan verilerinizin arkasına saklayarak korur. **TrueCrypt** biriminiz ortaya çıksa bile bu bilgiler korunaklı kalır. Bu kılavuz her iki tür birim hakkında da detaylı bilgi vermektedir.

## Offline Installation Instructions :

## TrueCrypt'i Kurma

- **Uygulamalı Rehberler'e Kısa Giriş** <sup>[1]</sup> bölümünü okuyun
- Aşağıdaki **TrueCrypt** ikonunu **tıklayın** ve kurucuyu \*Açın veya Çalıştırın. Gerekirse, kurucuyu kaydedin ve sonra bulup çift tıklayın\*
- Devam etmeden önce bir sonraki bölümdeki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulum gerçekleştikten sonra silebilirsiniz

TrueCrypt:



[44]

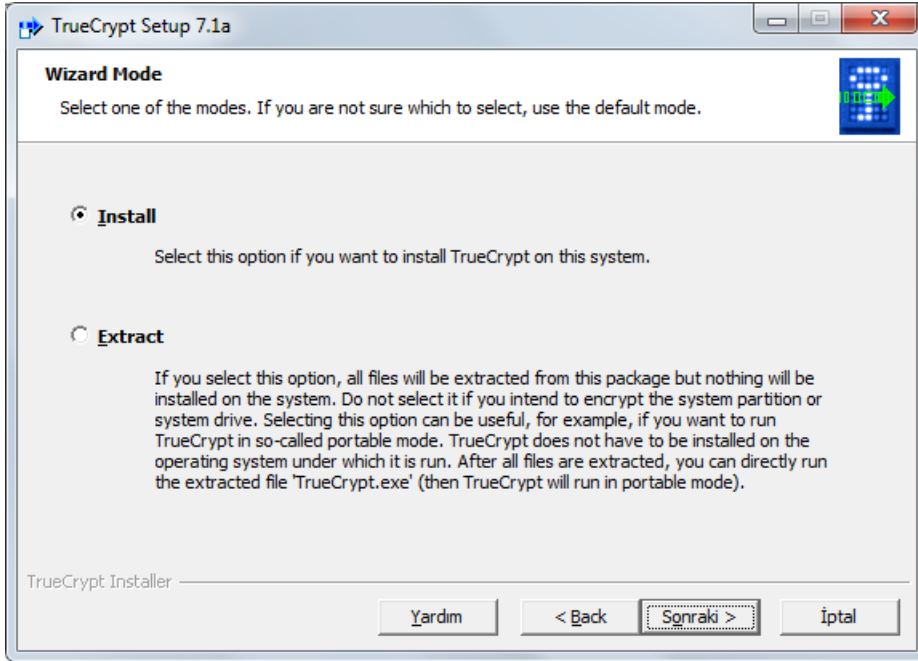
# TrueCrypt Nasıl Kurulur ve Standart bir Birim Nasıl Oluşturulur

Bu sayfadaki kısımların listesi:

- **2.0 TrueCrypt Nasıl Kurulur**
- **2.1 TrueCrypt Arayüzü Nasıl Türkçe'ye Çevrilir**
- **2.2 TrueCrypt Hakkında**
- **2.3 Standart Bir Birim Nasıl Oluşturulur**
- **2.4 Standart Bir Birim USB Hafıza Çubuğunda Nasıl Oluşturulur**
- **2.5 Standart Birim Nasıl Oluşturulur (Devamı)**

## 2.0 TrueCrypt Nasıl Kurulur

- 1. Adım.** TrueCrypt Setup 7.1a.exe 'ye çift tıklayın, Dosya Aç – Güvenlik Uyarısı kutusu açılabilir. Açılırsa, **TrueCrypt Lisans** ekranını etkinleştirmek için **Evet** 'i **tıklayın**.
- 2. Adım.** Sonraki düğmesini etkinleştirmek için *I accept and agree to be bound by the license terms* (Lisansın maddelerini kabul ediyorum) kutusunu **işaretleyin** ve aşağıda görünen ekranı etkinleştirmek için **Sonraki >** 'yi **tıklayın**.



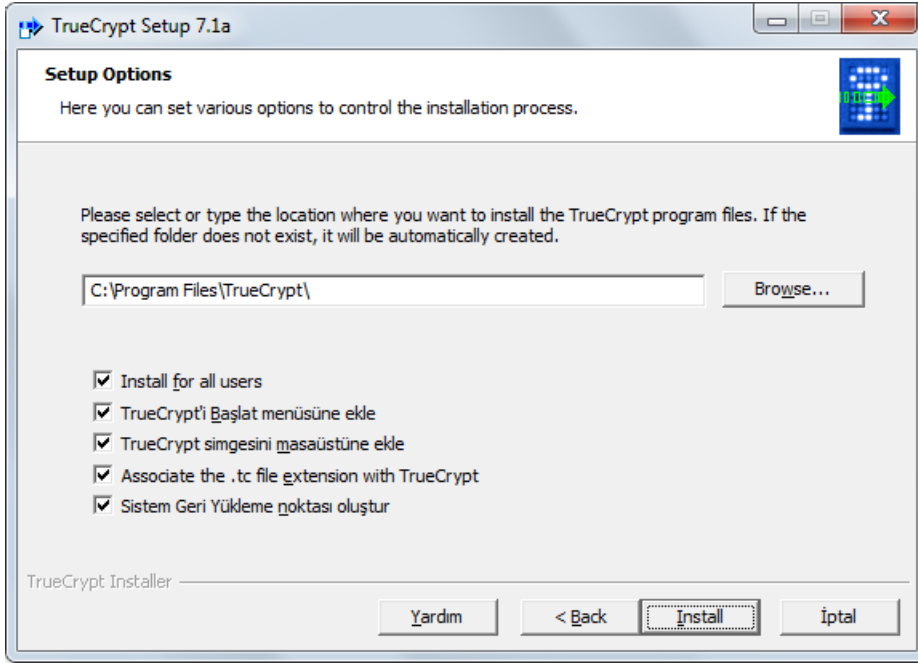
Şekil 1: Verili kurulum modunda Sihirbaz Modu Penceresi

- **Install Mode (Kurulum modu):** Bu seçenek, bilgisayarında **TrueCrypt** kullandıklarını saklama ihtiyacı hissetmeyen kullanıcılar içindir.
- **Extract Mode (Çıkarma modu):** Bu seçenek, **TrueCrypt**'i bilgisayarlarına yüklemek istemeyen ve USB hafıza çubuğunda taşınabilir bir **TrueCrypt** sürümü kullanmak isteyen kullanıcılar içindir.

**Not:** Çıkarma modu kullanıldığında zaman, tüm bölmeler veya sürücü şifreleme gibi bazı seçenekler çalışmayacaktır.

**Not:** Burada verili olan *Kurulum* modu önerilse de, daha sonra **TrueCrypt** taşınabilir modu da kullanabilirsiniz. **TrueCrypt Traveller** modu için lütfen **Taşınabilir TrueCrypt** <sup>[45]</sup> sayfasına bakınız.

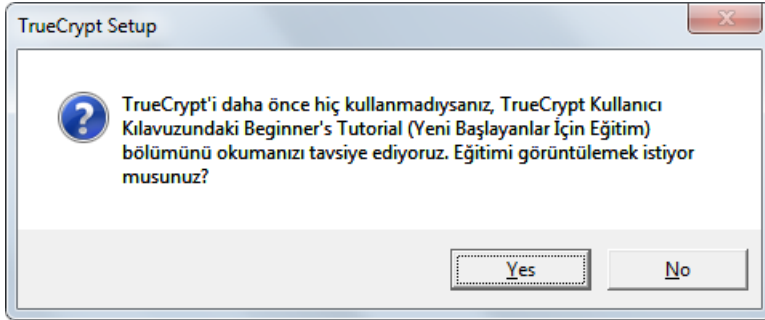
3. Adım. Aşağıda görünen ekranı etkinleştirmek için **Sonraki >** 'yi tıklayın:



Şekil 2: Kurulum Seçenekleri penceresi

4. Adım. Kurulum ekranını etkinleştirmek ve sisteminize **TrueCrypt**'i kurmaya başlamak için **Install** 'ı tıklayın.

5. Adım. Aşağıdaki ekranı etkinleştirmek için önce **OK** 'i, daha sonra da **Bitir** 'i tıklayın.



Şekil 3: TrueCrypt Kurulum onayı iletişim kutusu

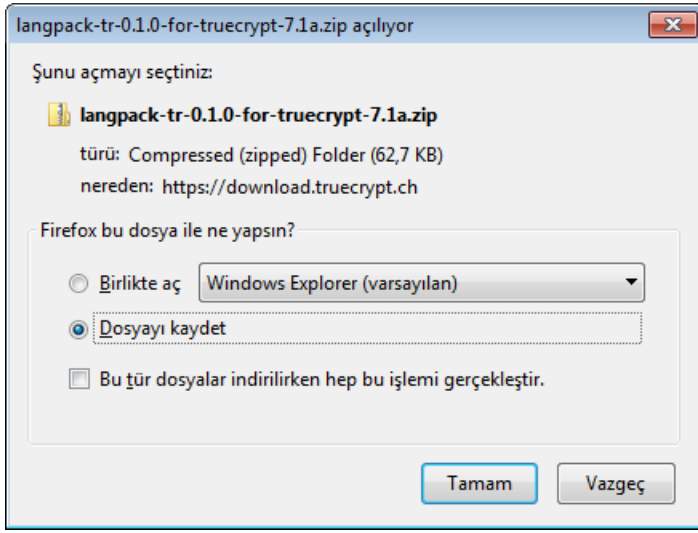
6. Adım. **TrueCrypt** kurulumunu bitirmek için **Yes** 'i tıklayın.

**Not:** Tüm kullanıcılara bu kılavuzu bitirdikten sonra **TrueCrypt** yardım belgelerine <sup>[46]</sup> bakmalarını öneririz.

## 2.1 TrueCrypt Arayüzü Nasıl Türkçe'ye Çevrilir

Her ne kadar mükemmel olmasa da **TrueCrypt** arayüzü Türkçe'ye çevrilmiştir. Aşağıdaki adımları takip ederek, TrueCrypt arayüzünü Türkçe görebilirsiniz:

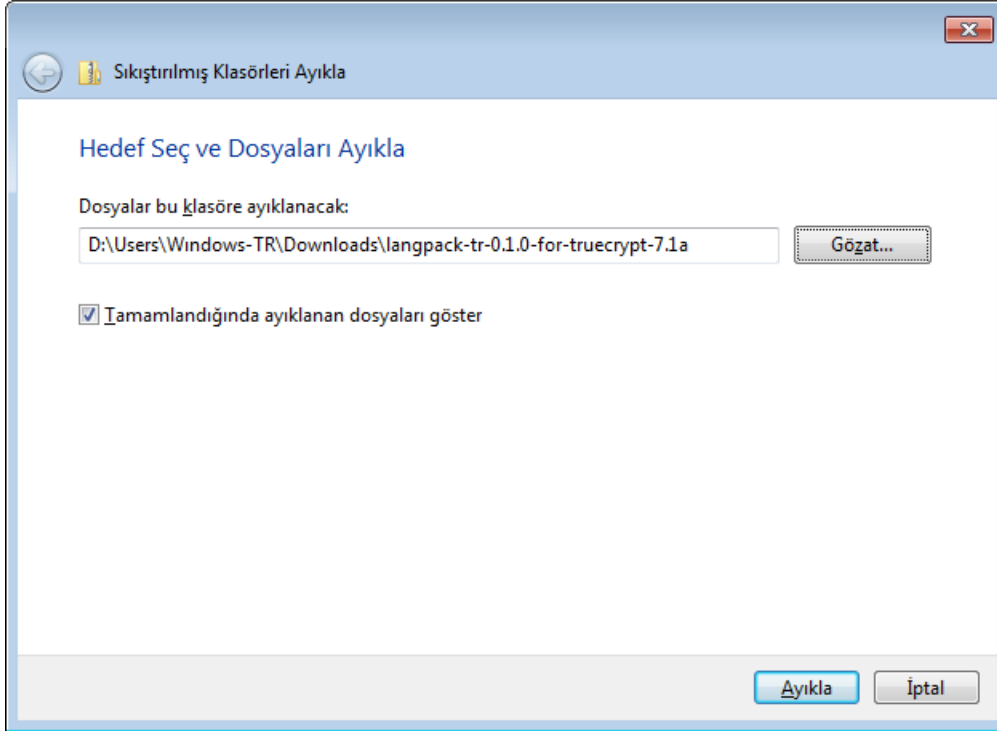
1. Adım. <https://truecrypt.ch/downloads/> <sup>[34]</sup> sayfasına gidin ve sayfayı tr-Turkish-Türkçe satırını görene kadar aşağı kaydırın. Bunun hizasındaki [langpack-uk-0.1.0-for-truecrypt-7.1a.zip](#) 'i tıklayın. Aşağıdaki ekran belirecektir



Şekil 4: Langpack-tr-0.1.0-for truecrypt-7.1.a.zip açılıyor ekranı

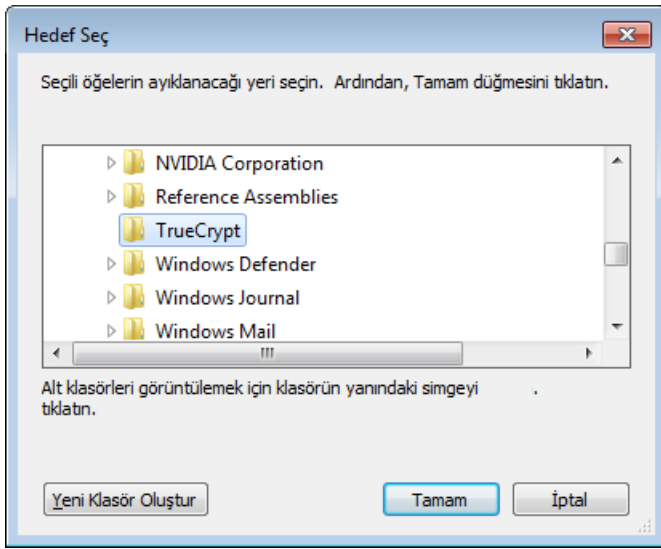
**2. Adım.** Dosyayı Kaydet'i seçip **Tamam** butonunu tıklayın.

**3. Adım.** İndirdiğiniz dosyayı **bulun** (mesela Karşıdan İndirilenler klasöründe), üzerine sağ tıklayın ve **Ayıkla** yı seçerek aşağıdaki ekranı açın:



Şekil 5: Sıkıştırılmış Klasörleri Ayıkla Ekranı

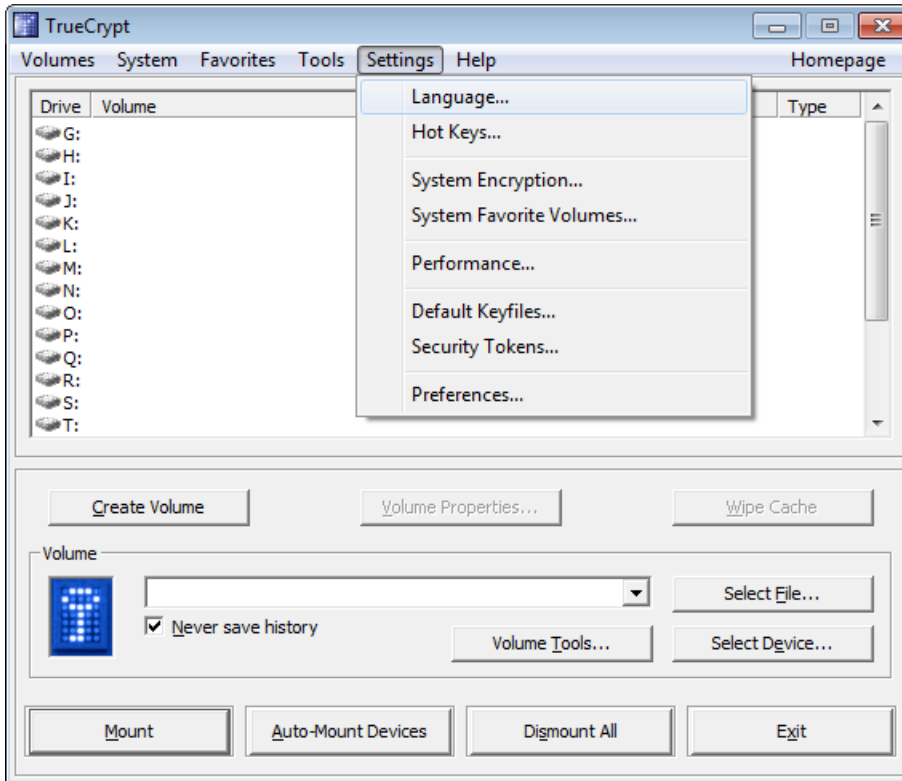
**4. Adım.** **Gözet...** butonunu tıklayarak **Hedef Seç** ekranını etkinleştirin. Aşağıda görüldüğü gibi **TrueCrypt.exe** dosyasının bulunduğu klasöre (mesela C:\Program Files\TrueCrypt) **ilerleyin**.



Şekil 6: Hedef Seç Ekranı

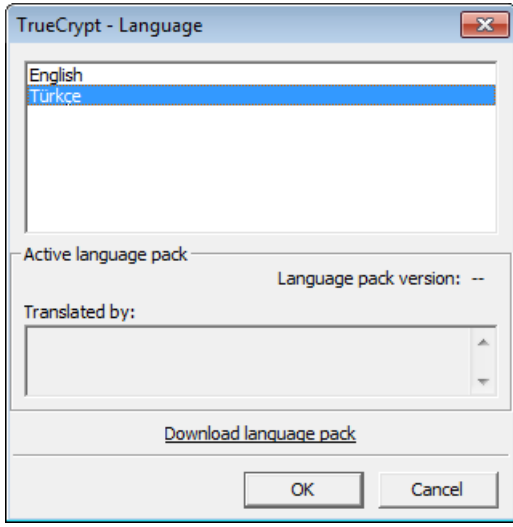
5. Adım. **Tamam** butonunu tıklayarak *Sıkıştırılmış Klasörleri Ayıkla Ekranı*'na geri dönün ve **Ayıkla** butonunu tıklayın. Güvenlik uyarısı belirirse **Devam** butonunu tıklayın.

6. Adım. TrueCrypt programını açın. Aşağıda görüldüğü gibi *Settings* (Ayarlar) ve *Language* (Dil) seçeneklerini tıklayın.



Şekil 7: Dil Ayarları Seçili TrueCrypt Ana Konsolu

6. Adım. Beliren pencerede aşağıda görüldüğü gibi Türkçe'yi seçin ve **OK** butonunu tıklayın.



Şekil 8: TrueCrypt - Language (Dil) Ekranı .

## 2.2 TrueCrypt Hakkında

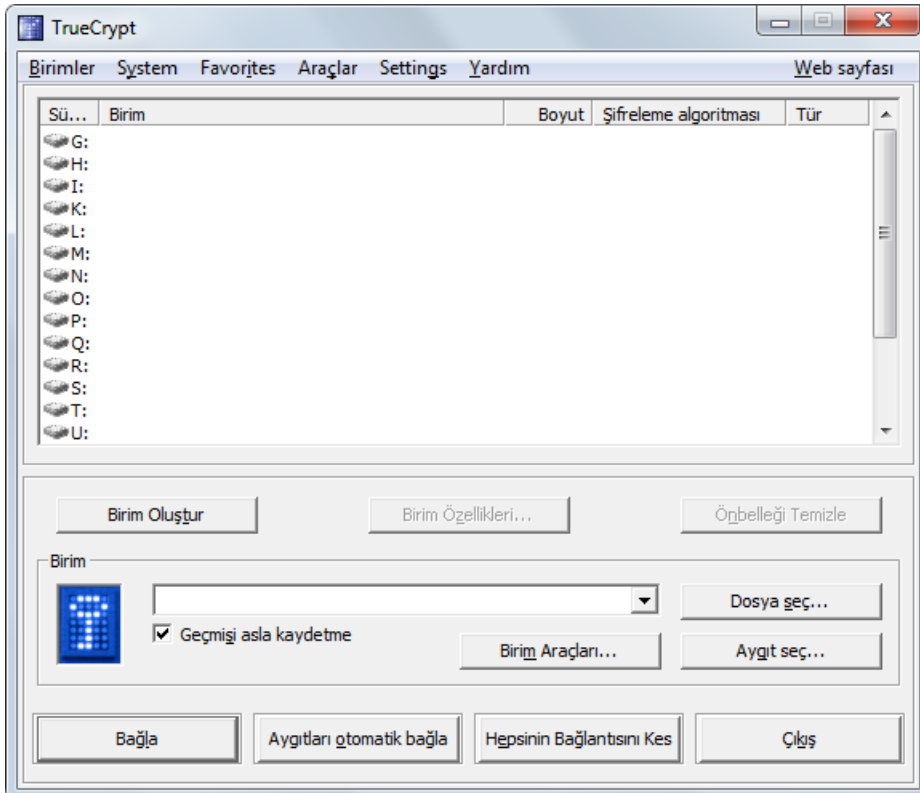
**TrueCrypt** dosyalarınızı, doğru şifreye sahip olmayan kimselerin onlara ulaşmasını engelleyerek, güvenli bir şekilde depolamanızı sağlar. Dosyalarınızı saklayan ve sadece doğru şifreye sahip olan kişinin açmasına olanak sağlayan elektronik bir kasa gibi çalışır. **TrueCrypt**, dosyalarınızı bilgisayarınızda güvenli bir şekilde kilitleyebileceğiniz *birimler* veya bölümler oluşturarak çalışır. Bu birimlerde veri oluşturduğunuz veya var olan verileri bu birimlere taşıdığınız zaman, **TrueCrypt** bu bilgileri otomatik olarak şifreleyecektir. Dosyalarınızı açtığınız veya dışarı çıkardığınızda, onları kullanabilmeniz için otomatik olarak şifrelerini çözecektir. Bu işleme *on-the-fly (anında) şifreleme* denir.

## 2.3 Standart Bir Birim Nasıl Oluşturulur?

**TrueCrypt** iki tür birim oluşturmaya olanak verir: *Gizli* ve *Standart*. Bu bölümde, dosyalarınızı depolayabileceğiniz bir *Standart Birim* oluşturma konusunda bilgi alacaksınız.

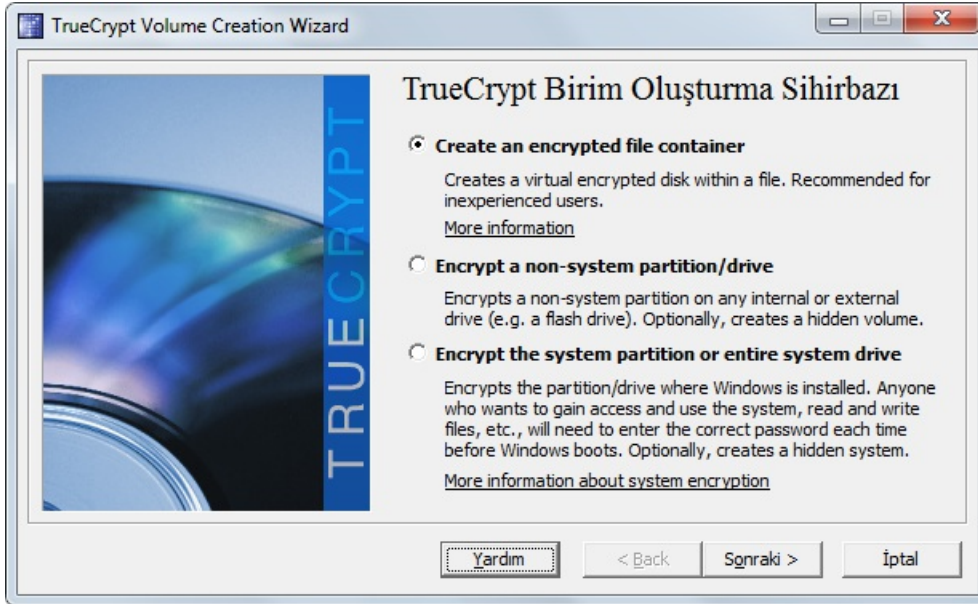
**TrueCrypt** kullanarak *Standart Birim* oluşturmak için aşağıdaki adımları takip edin: **1. Adım.**  e çift tıklayın veya **Başlat > Programlar > TrueCrypt > TrueCrypt'i seçin.**

**2. Adım.** **TrueCrypt** bölmesinde, aşağıda görüldüğü gibi bir sürücü **seçin**:



Şekil 9: TrueCrypt konsolu

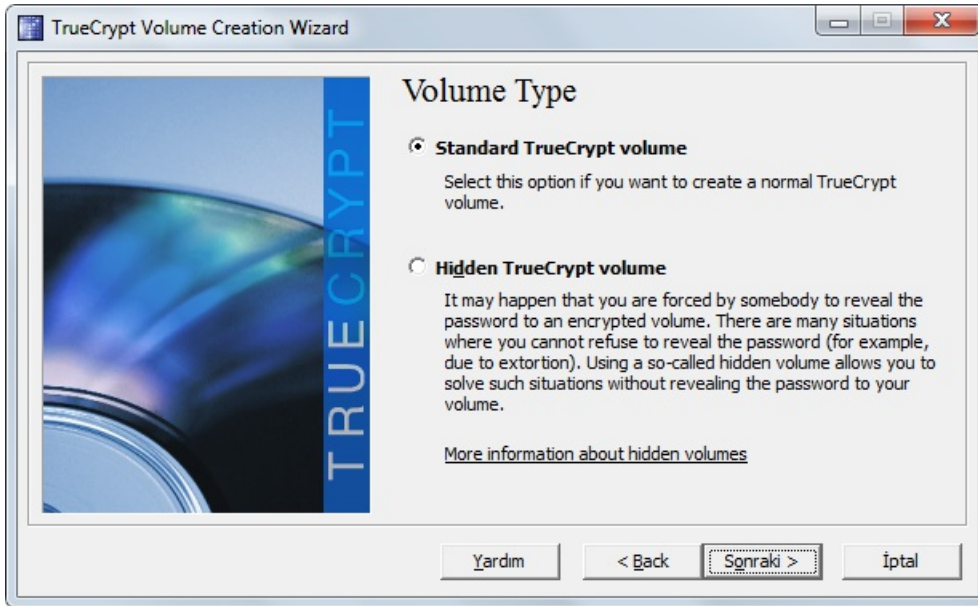
3. Adım. TrueCrypt Birim Oluşturma Sihirbazı'nı aşağıda görüldüğü gibi etkinleştirmek için **Birim Oluştur** butonuna tıklayın:



Şekil 10: TrueCrypt Birim Oluşturma Sihirbazı penceresi

Şekil 10'te görüldüğü gibi Standart Birim oluşturmak için üç seçenek vardır. Biz bu bölümde, *Create an encrypted file container* (Şifrelenmiş bir dosya kutusu oluştur) seçeneğini kullanacağız. Diğer iki seçenek ile ilgili bilgi için **TrueCrypt** [47] Birim Oluşturma Sihirbazı belgelerine başvurabilirsiniz.

4. Adım. Aşağıdaki ekranı etkinleştirmek için **Sıradaki >** butonuna tıklayın:



Şekil 11: Birim Tipi penceresi

TrueCrypt Birim Oluşturma Sihirbazı Birim Tipi penceresi Standart veya Gizli TrueCrypt birimi oluşturma tercihinizi belirlemenize olanak sağlar.

**Önemli:** Gizli Birim Oluşturma konusunda daha fazla bilgi için **Gizli Birim** [48] sayfasına başvurabilirsiniz.

5. Adım. *Standard TrueCrypt Volume* (Standart TrueCrypt Birimi) seçeneğini **işaretleyin**.

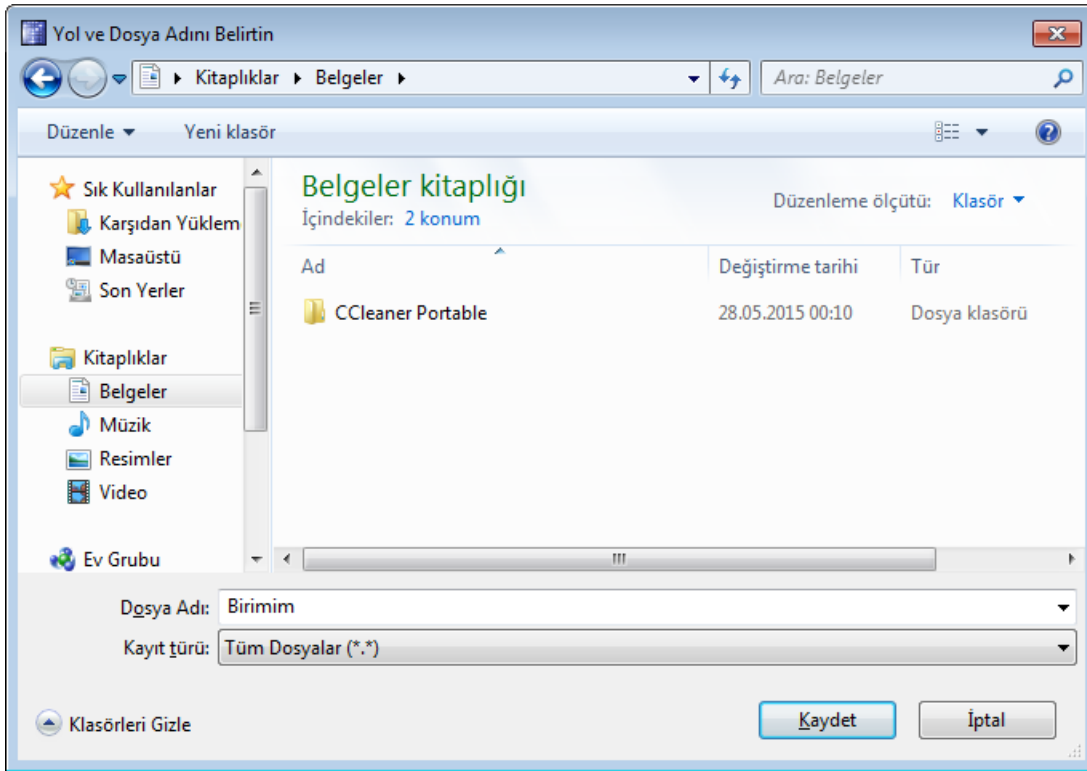
6. Adım. Aşağıdaki ekranı etkinleştirmek için **Sıradaki >** butonuna tıklayın:



Şekil 12: Birim Oluşturma Sihirbazı – Birim Yeri bölümü

Volume Creation Wizard - Volume Location (Birim Oluşturma Sihirbazı - Standart Birim) ekranında Standart Biriminizi nerede saklamak istediğinizi belirleyebilirsiniz. Bu dosya herhangi başka bir dosya gibi saklanabilir.

**7. Adım.** Dosyanın ismini metin kutusuna **yazın** veya aşağıdaki ekranı etkinleştirmek için **Dosya seç...** i tıklayın:



Şekil 13: Yol ve Dosya Adını Belirtin penceresi

**Not: TrueCrypt** Birimi normal bir dosyanın içine saklanır. Bu demektir ki, kopyalanabilir, yeri değiştirilebilir ve hatta silinebilir! Bu yüzden, dosyanın yerini ve ismini hatırlamanız çok önemlidir. Fakat, oluşturduğunuz birim için yeni bir isim seçmelisiniz (**USB Hafıza Çubuğunda Standart Bir Birim Nasıl Oluşturulur** kısmına başvurabilirsiniz). Bu kılavuzda, Standart Birimi **Belgelerim** klasöründe oluşturacağız ve ismini Şekil 8'de gördüğünüz gibi **Birimim** yapacağız.

**İpucu:** İstedığınız herhangi bir dosya ismini veya dosya uzantısını kullanabilirsiniz. Örneğin, Standart Biriminizi *tarifler.doc* olarak adlandırılabilir ve böylelikle herhangi bir Word belgesi gibi görünmesini sağlayabilirsiniz veya *tatiller.mpg* olarak adlandırıp bir film dosyası gibi gösterebilirsiniz.

**8. Adım.** Yol ve Dosya Adını Belirtin pencerelerini kapatmak ve aşağıda görüldüğü gibi **Birim Oluşturmama Sihirbazı** penceresine dönmek için **Kaydet** i tıklayın:



Şekil 14: Birim Yeri bölümünü gösteren TrueCrypt Birim Oluşturma Sihirbazı

9. Adım. Şekil 10'u etkinleştirmek için **Sonraki >** 'yi tıklayın.

## 2.4 Standart Bir Birim USB Hafıza Çubuğunda Nasıl Oluşturulur

USB hafıza çubuğunda **TrueCrypt Standart Birim** oluşturmak için, **2.2 Standart Bir Birim Nasıl Oluşturulur** kısmındaki 1'den 7'ye kadar olan adımları takip edin ve **Select a TrueCrypt Volume** (TrueCrypt Birimi Seçin) ekranını etkileştirin. Daha sonra, dosya yeri olarak **Belgelerim**'i değil USB hafıza çubuğunuzu **seçin**. Bir dosya adı **verin** ve **Standart Biriminizi** burada oluşturun.

## 2.5 Standart Bir Birim Nasıl Oluşturulur (Devamı)

Bu noktada, **Standart Biriminizde** saklanacak verilerinizi kodlamak için spesifik bir şifreleme yöntemi (ya da bu ekranda adlandırıldığı şekliyle **algoritma**) seçmeye hazırsınız.



Şekil 15: Birim Oluşturma Sihirbazı Şifreleme Seçenekleri bölümü

**Not:** Verili seçenekleri olduğu gibi kabul edebilirsiniz. Her iki seçenekte verilen algoritmalar oldukça güvenli kabul edilir.

10. Adım. TrueCrypt Birim Oluşturma Sihirbazı ekranını aşağıda görüldüğü gibi etkinleştirmek için **Sonraki >** 'yi tıklayın:

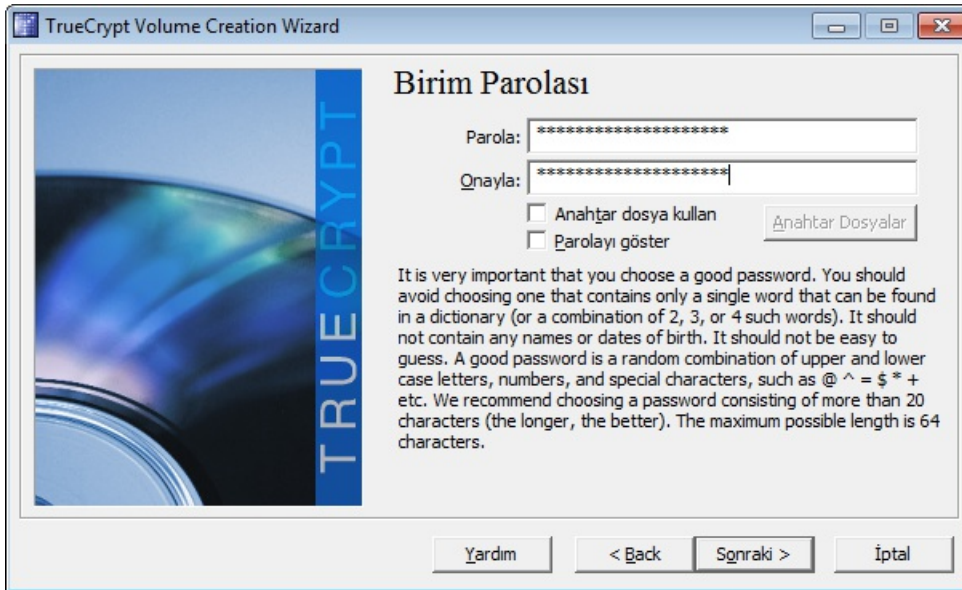


Şekil 16: Birim Boyutunu gösteren Birim Oluşturma Sihirbazı bölümü

**Volume Size (Birim Boyutu)** bölümü, \*Standart Biriminizi/ boyutunu belirlemenize olanak sağlar. Bu örnekte, 10 megabayt olarak belirlenmiştir. Fakat siz farklı bir boyut seçebilirsiniz. Depolamak istediğiniz belgelerin boyutunu ve dosya tiplerini göz önünde bulundurun ve buna uygun bir boyut seçin.

**İpucu:** Standart Biriminizi daha sonra bir CD'ye yedeklemek istiyorsanız boyutu 700MB veya daha küçük seçmelisiniz.

**11. Adım.** Metin alanına belirlediğiniz birim boyutunu **girin** ve aşağıdaki ekranı etkinleştirmek için **Sonraki >** 'yi **tıklayın**:



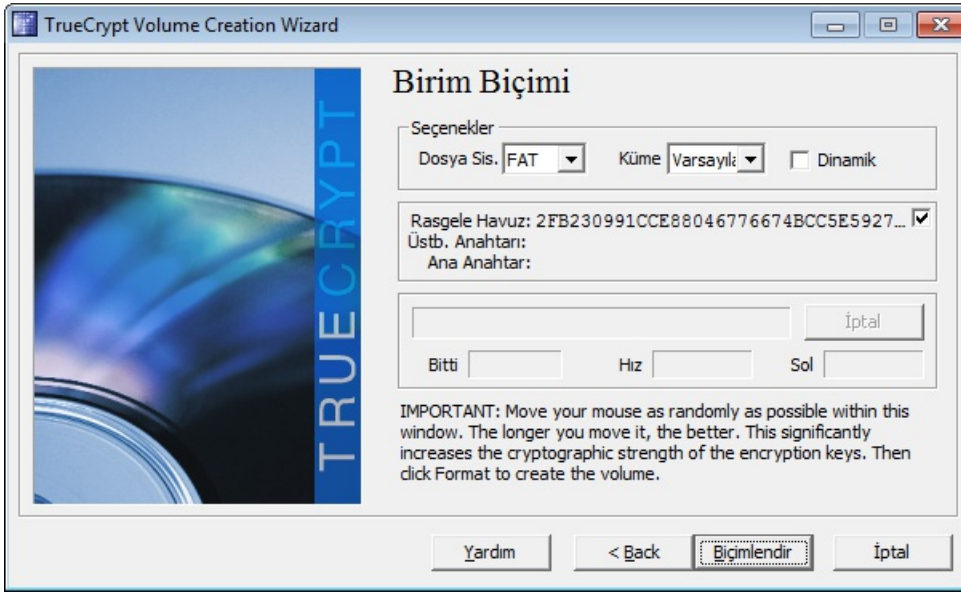
Şekil 17: Birim Şifresini gösteren TrueCrypt Birim Oluşturma Sihirbazı bölümü

**Önemli:** Standart Birim oluştururken yapmanız gereken en önemli işlemlerden biri güvenli ve güçlü bir şifre yaratmaktır. İyi bir şifre şifrelenmiş biriminizi korur, bu yüzden ne kadar güçlü bir şifre seçerseniz o kadar güvende olursunuz. Şifrenizi kendiniz belirlemek ve hatırlamak zorunda değilsiniz. Bunun yerine, **KeePass** gibi bir program kullanabilirsiniz. Şifre yaratma ve depolama konusunda daha fazla bilgi için ([KeePass'e](mailto:KeePass@tr/keepass_main)) bakın.

**12. Adım.** Şifrenizi ilgili kutuya ve daha sonra bir kez daha *Confirm* (Onayla) kutusuna **yazın**.

**Önemli:** Her iki şifre aynı olmadığı sürece *Sonraki* düğmesi etkinleşmeyecektir. Şifreniz güvenli değilse bu konuda bir uyarı mesajı alacaksınız. Böyle bir durumda şifrenizi değiştirin! **TrueCrypt** seçeceğiniz herhangi bir şifre ile çalışacak olsa da, şifreniz güçlü değilse verileriniz güvende olmaz.

**13. Adım.** Aşağıdaki ekranı etkinleştirmek için **Sonraki >** 'yi **tıklayın**:



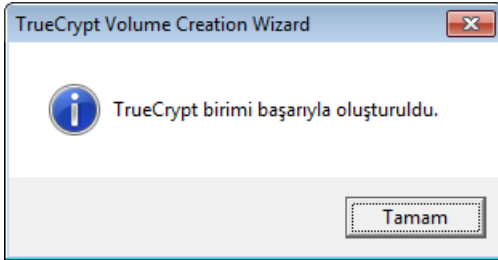
Şekil 18: Birim Formatı gösteren TrueCrypt Birim Oluşturma Sihirbazı bölümü

**TrueCrypt**, Standart Birim oluşturmaya hazırdır. İmlecinizi *TrueCrypt Birim Oluşturma Sihirbazı* penceresinde birkaç saniye dolaştırın. İmleci ne kadar uzun süre dolaştırırsanız şifreleme kodlarınız o kadar kuvvetli olacaktır.

**14. Adım.** Standart biriminizi oluşturmak için **Biçimlendir** i tıklayın.

**TrueCrypt**, daha önce belirlendiği üzere *Belgelerim* klasöründe *Birimim* adlı bir dosya oluşturacaktır. Bu dosya, 10 megabayt büyüklüğünde bir **TrueCrypt Standart Birim** oluşturacak ve dosyalarınızı güvenli bir şekilde burada saklamanıza olanak sağlayacaktır.

*Standart Birim* başarılı bir şekilde oluşturulduktan sonra, aşağıdaki iletişim kutusu görünür:



Şekil 19: TrueCrypt birimi başarılı bir şekilde oluşturuldu mesajı ekranı

**15. Adım.** *Standart Birim* oluşturmaya tamamlamak ve **TrueCrypt** konsoluna geri dönmek için **Tamam** i tıklayın.

**16. Adım.** *TrueCrypt Birim Oluşturma Sihirbazı* nı kapatmak için **Sonraki >** i tıklayın.

## gpg4usb – E-posta Metni ve Dosya Şifreleme

### Short Description:

**gpg4usb** metin (e-posta) iletilerini ve dosyalarını şifreleme işlevine sahip, ücretsiz, açık kaynak, taşınabilir bir programdır. **GPG** ve **PGP** programları gibi Açık Anahtar Şifreleme algoritmaları kullanır.

### Online Installation Instructions:

#### gpg4usb'yu indirme

- <http://www.gpg4usb.org/download.html> web sayfasını açmak için aşağıdaki **gpg4usb** ikonuna tıklayın
- \*zip arşivini indirmeye gitmek için **File Name** altındaki **gpg4usb-x.x.x.zip** bağlantısına tıklayın
- **gpg4usb-x.x.x.zip** dosyasını **bulun** ve **ayıklayın**
- Tüm dosyaları ayıkladıktan sonra, bilgisayarınıza kaydettiğiniz .zip dosyasını silebilirsiniz

#### gpg4usb

## Ana Sayfa

- <http://www.gpg4usb.org/> [50]

## Bilgisayar Gereksinimleri

- Tüm Windows sürümleri

## Bu kılavuzda kullanılan sürümler

- 0.3.3

## Bu bölümün son güncellenme tarihi

- Temmuz 2014

## Lisans

- Özgür ve Açık Kaynak Yazılım

## Gerekli Okuma

- Nasıl Yapmalı Kitapçığı'nın **7. İnternet iletişiminizin gizliliği nasıl korunur** [51] bölümü
- **\*\*İnsan Hakları Koruyucuları için Dijital Güvenlik ve Gizlilik\*\*** [52], **2.4 Kriptoloji – Açık Anahtar Şifreleme** bölümü (38. Sayfa)

## Buradan sağlayacağınız faydalar::

- Nerede olursanız olun (örneğin İnternet kafe veya iş), dosya ve yazılı iletilerinizi şifreleyebilme
- İletilerinizi çevrim dışı olduğunuz veya İnternet erişiminizin olmadığı durumlarda şifreleyebilme ve daha sonra İnternet bağlantısı olan bir bilgisayardan gönderebilme

## 1.1 Başlamadan önce bu araç hakkında bilmeniz gerekenler

**gpg4usb** yazılı ileti ve dosyaları şifrelemenize ve şifrelerini çözmenize olanak veren, basit, hafif ve taşınabilir bir programdır. **gpg4usb**, **açık-anahtar kriptografisi** ile çalışır. Bu yöntemle, her kullanıcı kendi **anahtar çiftini** oluşturmaktadır. İlk anahtar **kişisel anahtar** olarak bilinir. Bir parola veya şifreyle korunur ve asla kimseyle paylaşılmamalıdır.

İkinci anahtar **açık anahtar** olarak bilinir. Bu anahtarı iletişimde olduğunuz insanlarla paylaşabilirsiniz ve onlar da kendi açık anahtarlarını sizinle paylaşabilir. Birisinin açık anahtarını edindiğiniz anda ona şifreli mesajlar göndermeye başlayabilirsiniz. Uyumlu olan tek açık anahtara sahip olan bu kişi olduğu için, şifreli mesajlarınızı okuyabilecek olan tek kişi de odur.

Aynı şekilde, kendi açık anahtarınızı e-posta ile iletişime geçtiğiniz kişilere gönderir ve onunla eşleşen açık anahtarı saklarsanız, bu kişilerden gelecek şifreli mesajları okuyabilecek tek kişi de siz olursunuz.

Ayrıca, mesajlarınıza dijital imza da ekleyebilirsiniz. Sizin açık anahtarınıza sahip olan ve mesajınızı alan kişi bu sayede e-postanın sizden geldiğini onaylayabilir ve içeriğinin değiştirilmediğinden emin olabilir. Aynı şekilde, karşı tarafın açık anahtarına sahipseniz, onun mesajlarındaki dijital imzayı kontrol edebilirsiniz.

**gpg4usb** ile şifreleme anahtar çifti oluşturabilir, açık anahtarı başkalarıyla paylaşmak üzere çıkarabilir, yazılı mesaj oluşturup onu şifreleyebilirsiniz. Açık anahtarı ya/ya da şifrelenmiş mesajı **gpg4usb'ten** kendi e-postanıza kopyalayıp yapıştırabilirsiniz ya da daha sonra göndermek üzere metin dosyası olarak kaydedebilirsiniz. Belge ve dosyalar da şifrelenebilir.

**Not:** Aklınızda tutun ki, belge ve dosyalarınızın orijinal, şifrelenmemiş versiyonları bilgisayarınızda durmaya devam eder. Bu yüzden, hem siz hem de iletişimde olduğunuz kişiler, gerektiği zaman bunları bilgisayardan silmeyi unutmamalıdır.

**gpg4usb**, benzer **GPG** ve **PGP** programları ile anahtar ve şifrelenmiş mesaj takası yapmanıza izin verir.

## Offline Installation Instructions :

### gpg4usb'yi indirme

- Aşağıdaki **gpg4usb** ikonunu **tıklayarak** zip arşivi dosyasını bilgisayarınıza kopyalayın
- **gpg4usb.zip** dosyasını **bulun** ve **ayıklayın**
- Tüm dosyaları ayıkladıktan sonra, bilgisayarınıza kaydettiğiniz **gpg4usb.zip** dosyasını silebilirsiniz.

## gpg4usb

# gpg4usb Nasıl Kurulur ve Anahtar Çifti Nasıl Oluşturulur?

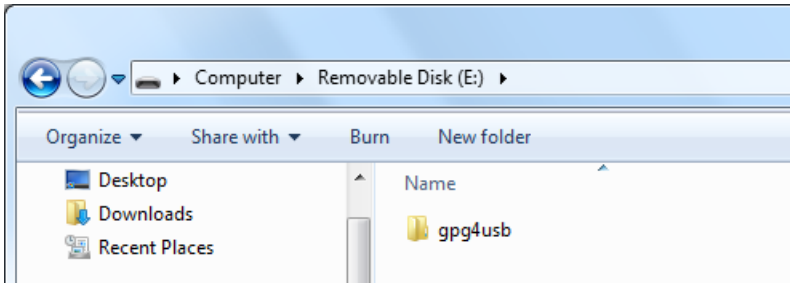
Bu sayfadaki bölümlerin listesi:

- [2.0 gpg4usb Nasıl Kurulur?](#)
- [2.1 gpg4usb Kullanarak Nasıl Anahtar Çifti Oluşturulur?](#)

## 2.0 gpg4usb Nasıl Kurulur?

**gpg4usb** taşınabilir bir alettir ve bilgisayarınıza kurmanız gerekmez. Yazılım sıkıştırılmış dosyada dağıtılır ve doğrudan USB sürücüsüne veya bilgisayarınızdaki bir dosyaya ayıklanır. Başlamak için aşağıdaki adımları takip ediniz:

**1. Adım. gpg4usb** sıkıştırılmış arşiv dosyasını bulun ve içeriğinin tümünü taşınabilir USB sürücüsüne veya bilgisayarınızdaki bir klasöre **ayıklayın**:



Şekil 1: gpg4usb programı hedef klasör yeri

## 2.1 gpg4usb Kullanarak Anahtar Çifti Nasıl Oluşturulur?

E-posta, yazılı ileti, belge ve dosyalarınızı şifreleme ve şifrelerini çözmeye başlamak için, öncelikle iki işlem gerçekleştirmelisiniz. Öncelikle şifreleme anahtar çifti oluşturmalı veya taşımalsınız, sonra da iletişimde olacağınız kişilere açık anahtarınızı göndermeli ve onlarınkini edinmeli ve kendi anahtarlığınıza eklemelisiniz. Açık anahtarların nasıl paylaşıldığını bir sonraki bölümde anlatacağız. **gpg4usb**, programı ilk başlattığınız zaman anahtar çifti oluşturmanıza yardımcı olur. Başlangıç (Getting Started) penceresine her zaman *Yardım -> Sihirbazı Aç (Help -> Open Wizard)* menüsüne her zaman gidebilirsiniz.

**1. Adım. gpg4usb** programını ilk defa çalıştırmak için, önce **gpg4usb**'yi **bulup** üstüne **çift tıklayın** ve **gpg4usb** klasörünü açın ve **! [54]**'e **çift tıklayın**. bu şekilde *Getting Started* (Başlangıç) penceresini etkinleştireceksiniz. Bir dil seçin ve *Next*'i (İleri'yi) **tıklayın** (Bu programın ne yazık ki Türkçe sürümü henüz yoktur).

**2. Adım. Choose your Action** (Eyleminizi Seçin) ekranında, *Create a new keypair*'i (Yeni bir anahtar çifti oluştur'u) **tıklayın**.



Şekil 2: Eyleminizi Seçin

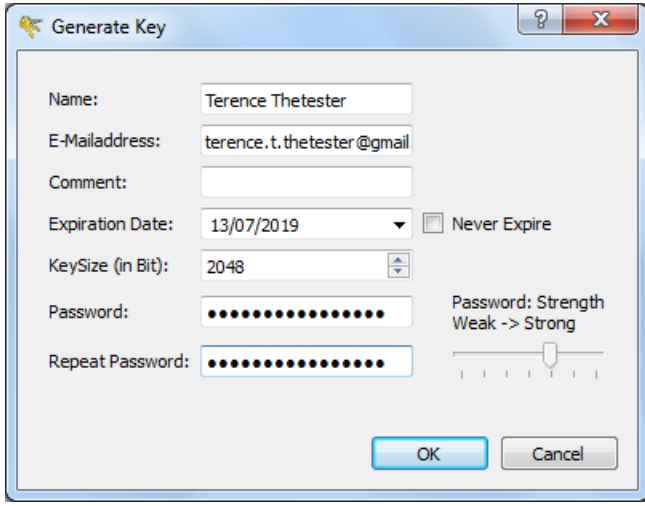
İlk Başlangıç Sihirbazı ekranında var olan anahtarları buraya taşıma seçeneklerini bulabilirsiniz. Eğer **gpg4usb**'yi güncelliyorsanız, *import settings and/or keys from **gpg4usb**'yi (gpg4usb'den* ayarları ve/veya anahtarları aktarı) seçebilirsiniz. *Enigmail ile Thunderbird* <sup>[55]</sup> kullanıyorsanız, *import keys from GnuPG* (GnuPG'den anahtarları taşı) seçeneğini seçebilirsiniz. *Help -> Open Wizard* (Yardım -> Sihirbazı Başlat) menüsünden sihirbazı çalıştırarak anahtarlarınızı daha sonra da taşıyabilirsiniz.

**3. Adım.** *Create a keypair*'de (Anahtar çifti oluştur'da) *Create New Key*'i (Yeni Anahtar Oluştur'u) **tıklayın**.



Şekil 3: Yeni Anahtar Oluştur

**4. Adım.** İlgili metin alanlarına verileri **girmenizden** sonra pencereniz aşağıdakine benzeyecektir:



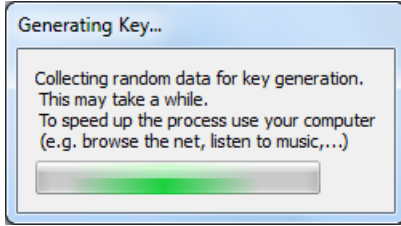
Şekil 4: Doldurulmuş Anahtar Oluşturma formu örneği

**Önemli:**

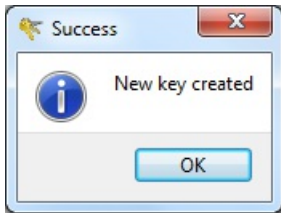
- Kişisel anahtarınızı korumak için güvenli bir şifre oluşturun (lütfen **3. Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** <sup>[4]</sup> bölümüne bakın).
- Expiration date (Zaman aşımına uğrama) seçeneğini seçip 5 yıldan daha az bir süreye ayarlamanızı öneririz.
- En az 2048 bit büyüklüğünde anahtarlar oluşturmaları şiddetle tavsiye ederiz. Daha büyük anahtarlar daha güvenlidir ama oluşturma, metinleri şifrelemesi ve şifre çözmesi daha çok zaman alır.

**Not:** Anahtarınızı oluştururken gerçek isminizi ve gerçek e-posta adresinizi kullanmanız gerekmez. Fakat, iletişim kuracağınız hesabın e-posta adresini kullanmanız, iletişim kuracağınız kişilerin anahtarınızı bu hesap ile bağlantılandırmasını kolaylaştırır.

**6. Adım.** Anahtar çiftini oluşturmak için **OK**'i (Tamam'ı) **tıklayın**.

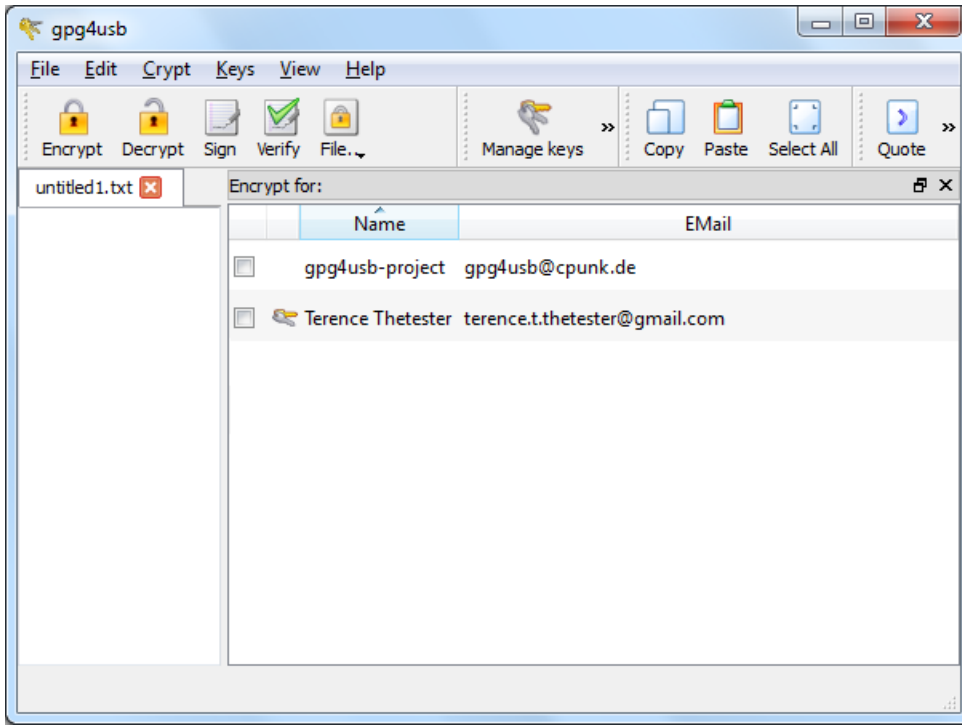


Şekil 5: Anahtar Oluşturuluyor...



Şekil 6: Yeni Anahtar Oluşturuldu

**7. Adım.** **gpg4usb** penceresine geri dönmek için **OK**'i (Tamam'ı) **tıklayın**. Anahtar çifti başarı ile oluşturulduktan sonra, aşağıdaki benzer bir ekran göreceksiniz:



Şekil 7: Yeni oluşturulmuş anahtar çiftini gösteren gpg4usb penceresi

Anahtar çiftinizi oluşturduğunuza göre, açık anahtarınızı diğer insanlarla nasıl paylaşacağınızı ve onların açık anahtarlarını nasıl taşıyacağınızı öğrenebilirsiniz.

## Anahtarlar Nasıl Gönderilir ve Alınır?

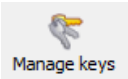
Bu sayfadaki bölümlerin listesi:

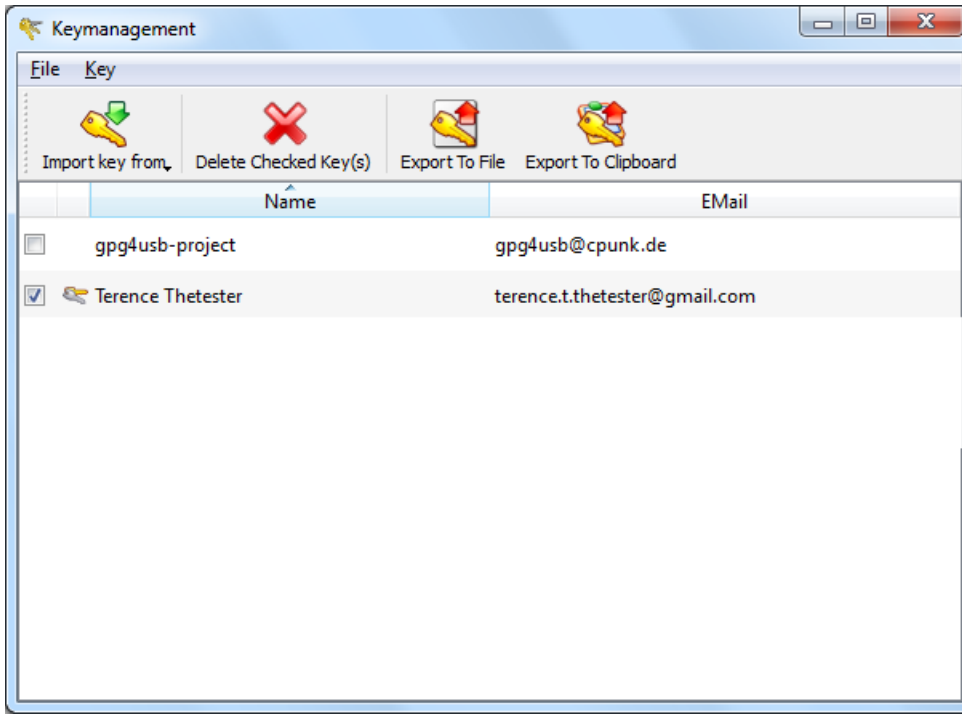
- [3.1 Açık Anahtarınızı gpg4usb Kullanarak Nasıl Gönderirsiniz](#)
- [3.2 İletişimde Olduğunuz Kişinin Açık Anahtarını gpg4usb Kullanarak Nasıl İçer Aktarırsınız](#)
- [3.3 Bir Açık Anahtarı gpg4usb Kullanarak Nasıl Doğrularsınız](#)

### Açık Anahtarınızı gpg4usb Kullanarak Nasıl Gönderirsiniz

İletişim kurduğunuz kişilerin size şifreli mesaj gönderebilmesi için onlara açık anahtarınızı göndermeniz gerekir.

Açık anahtarınızı **gpg4usb** kullanarak göndermek için aşağıdaki adımları takip ediniz:

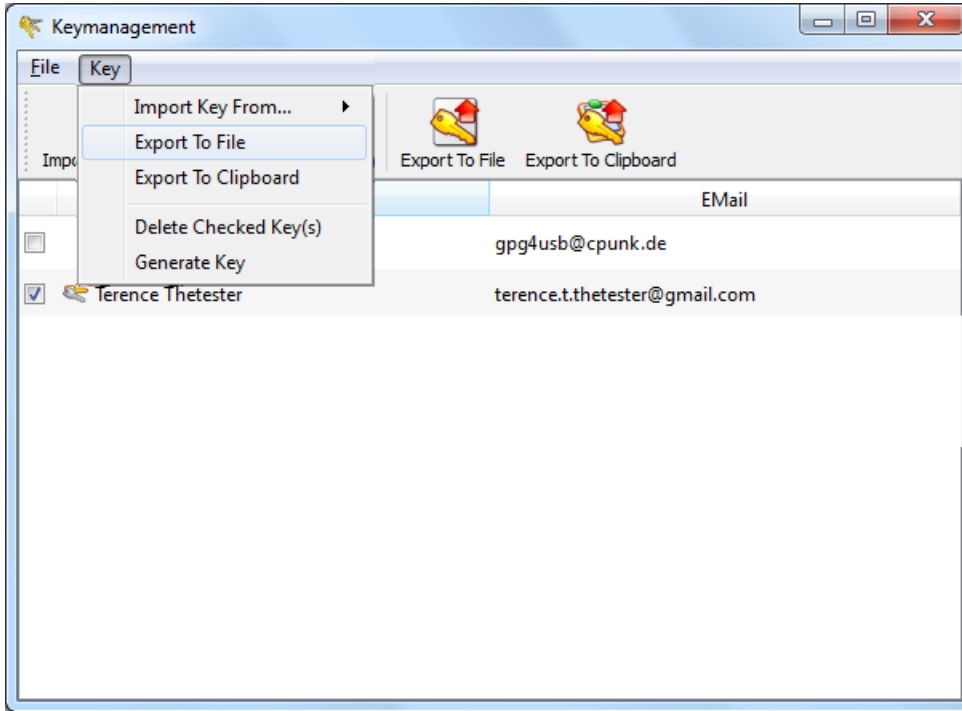
1. **Adım.** **gpg4usb** klasörünü açmak için  **gpg4usb**'ye **çift tıklayın**.
2. **Adım.** **gpg4usb** programını açmak için  **start\_windows.exe**'ye **çift tıklayın**.
3. **Adım.** Aşağıdaki ekranı etkinleştirmek için  **Manage keys** 'e **tıklayın**.



Şekil 1: Tüm anahtar çiftlerini gösteren Anahtar düzenleme penceresi

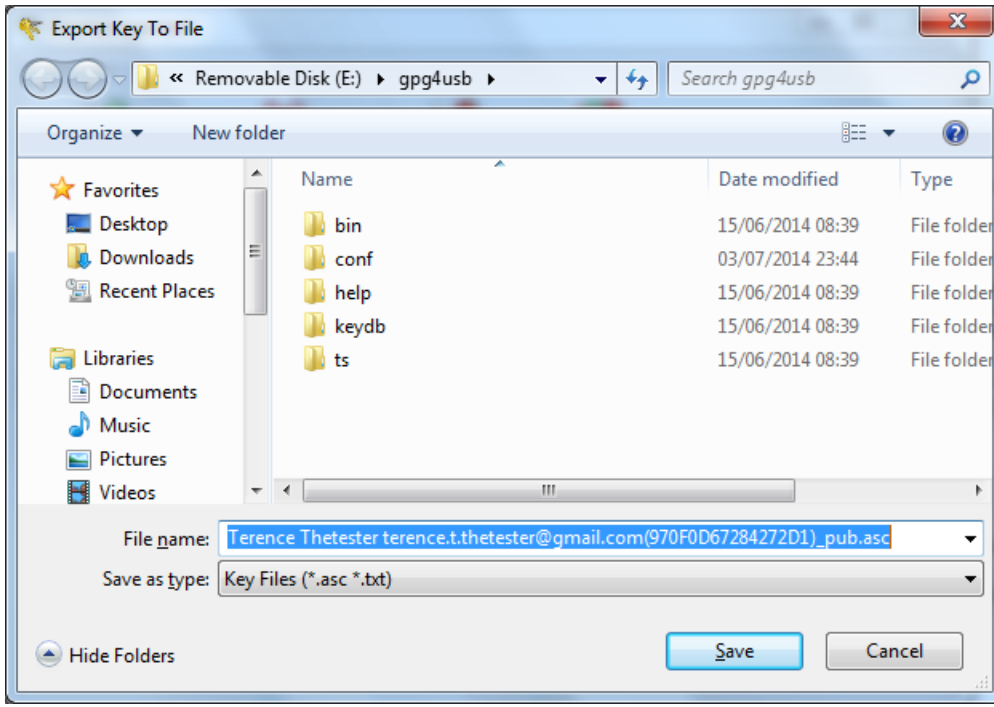
3. Adım. Yukarıdaki **Şekil 1**'de görüldüğü gibi kendi anahtarınızı işaretleyin.

4. Adım. Aşağıda görüldüğü gibi **Key**(Anahtar) menüsünden *Export To File*'i (Dosyaya Aktar)'ı seçin:

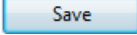


Şekil 2: Dosyaya Aktar seçeneği seçili Anahtar düzenleme penceresi

Bu sayede aşağıdaki ekran etkinleşecektir:



Şekil 3: Dosyaya Aktar tarayıcı penceresi

5. Adım. Anahtar çiftinizi **pgp4usb** program klasörüne kaydetmek için 'i tıklayın.

6. Adım. Açık anahtarınızı içeren dosyayı istediğiniz kişiye ek dosya olarak **gönderin**.

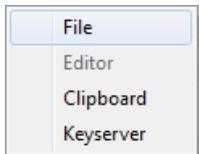
## 3.2 İletişimde Olduğunuz Kişinin Açık Anahtarını pgp4usb Kullanarak Nasıl İçe Aktarırsınız?

Bilgileri şifreleyip iletişimde olduğunuz kişiye göndermeden önce, onun açık anahtarını elinizde bulundurmalısınız. İletişimde olduğunuz kişinin açık anahtarını **pgp4usb** kullanarak içe aktarmak için aşağıdaki adımları takip edin:

1. Adım. **pgp4usb** programını açmak için  **start\_windows.exe**'e **çift tıklayın**.

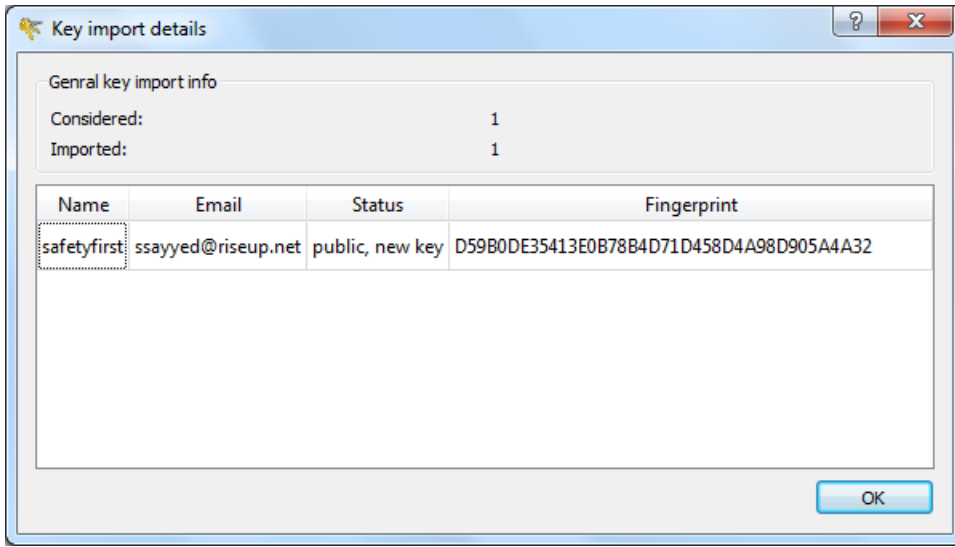


2. Adım. Aşağıdaki ekranı etkinleştirmek için 'i **tıklayın**:



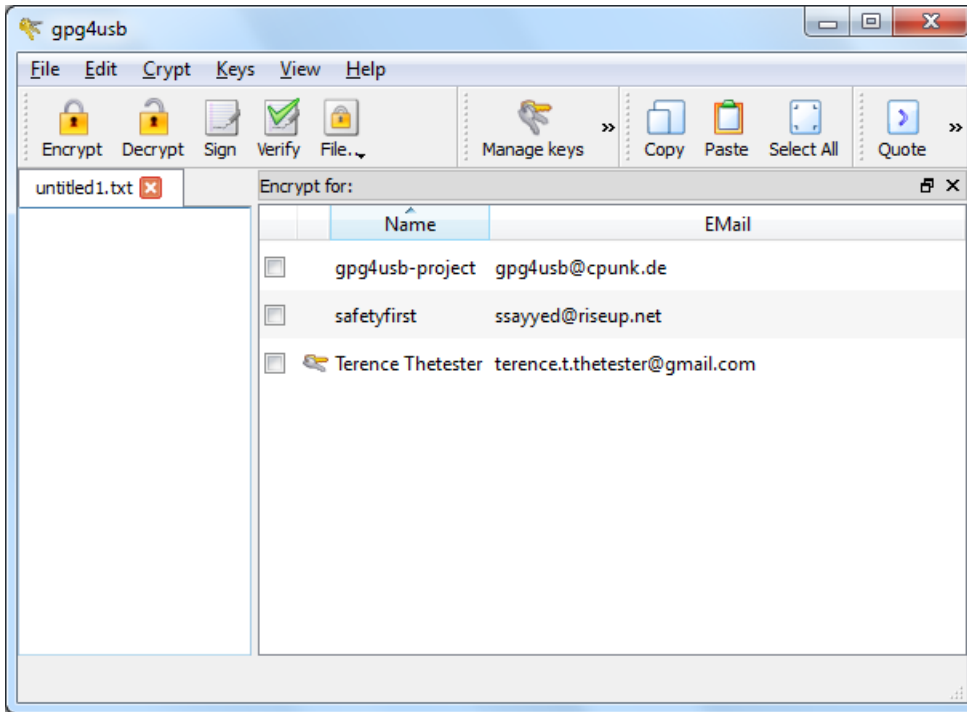
Şekil 4: Anahtarı İçe Aktar iletişim kutusu

3. Adım. Almak istediğiniz anahtarı **bulun** ve **seçin**.



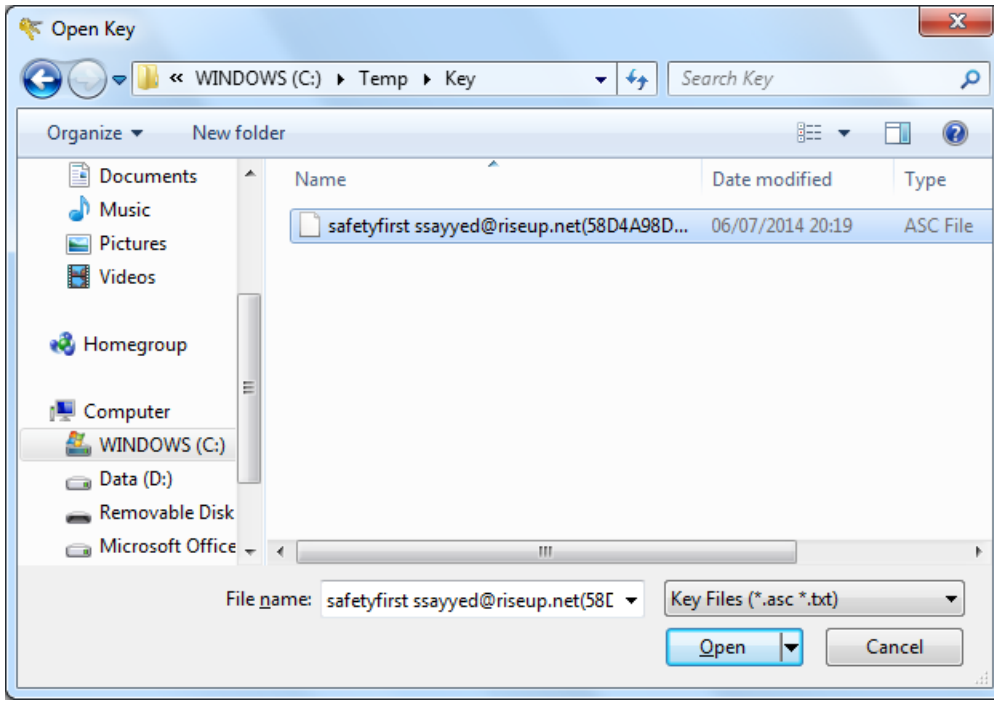
Şekil 5: Açık Anahtar

4. Adım. Aşağıdaki ekranı etkinleştirmek için *Open'ı* (Aç'ı) **tıklayın**.



Şekil 6: Anahtar İçe Aktarma Detayları

5. Adım. Yukarıdaki pencereyi kapatmak için *OK'i* (Tamam'ı) **tıklayın** ve **gpg4usb** ana penceresine geri dönün. Yeni içe aktarılmış anahtar aşağıdaki gibi görünecektir.



Şekil 7: Yeni içe aktarılmış iletişim kuracağınız kişinin hesabına bağlı olan açık anahtarı gösteren gpg4usb konsolu

İletişim kuracağınız kişinin açık anahtarını başarı ile içe aktardınız. Şimdi bu anahtarı doğrulayabilir ve imzalayabilirsiniz.

### 3.3 Bir Açık Anahtarı gpg4usb Kullanarak Nasıl Doğrularsınız?

Alınan anahtarın gerçekten onu gönderen kişiye ait olup olmadığını doğrulamanız gerekir. İçe aktardığınız her açık anahtar için siz ve iletişimde olduğunuz kişiler bu önemli işlemi tekrarlamalısınız.

Anahtar çiftini doğrulamak için aşağıdaki adımları takip edin::

**1. Adım.** İletişim kuracağınız kişi ile e-posta haricinde başka bir kanaldan **temas kurun**.

**Not:** Telefon, yazılı mesaj, **Voice over Internet Protocol (VoIP)** veya başka bir yöntem kullanabilirsiniz, fakat bunları iletişim kuracağınız kişinin gerçekten o olduğundan emin iseniz yapın. Güvenli bir şekilde ayarlandıkları zaman, telefon görüşmeleri ve yüz yüze buluşmalar kişinin kimliğini doğrulamanız için en güvenli yöntemlerdir.

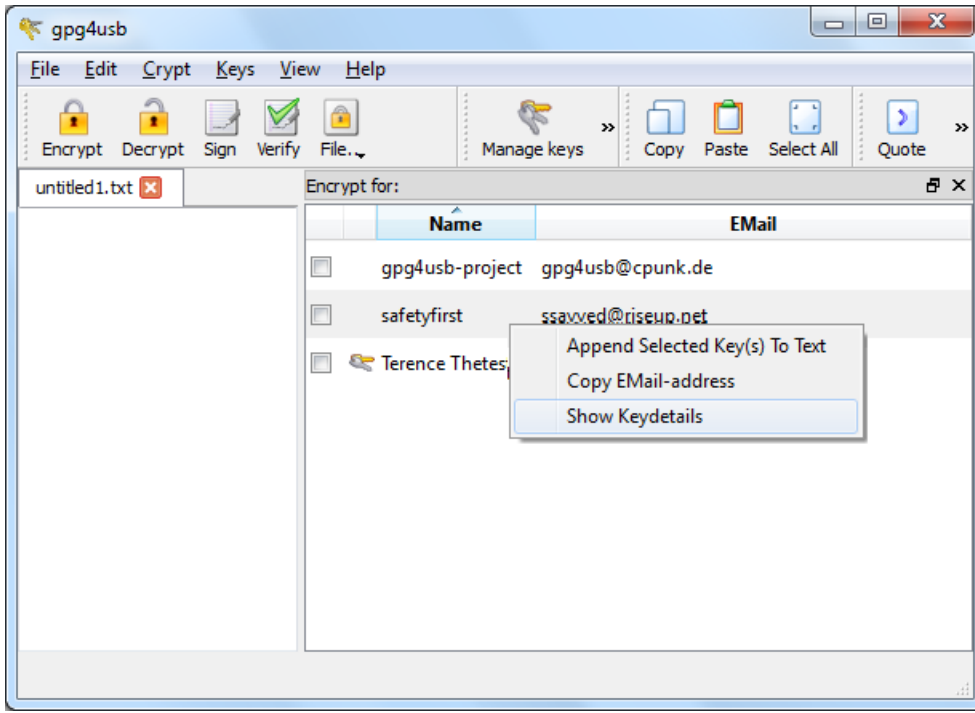
**2. Adım.** Siz ve iletişim kurduğunuz kişi değiştiğiniz açık anahtarların 'parmak izlerini' doğrulamalısınız.

**Not:** Parmak izi, her anahtarın sahip olduğu kendine özgü sayı ve harflerdir. Parmak izinin kendisi gizli değildir, daha sonra, gerektiği zaman doğrulama işlemi için kullanılmak üzere kaydedilebilir.

Yarattığınız veya aldığınız açık anahtarların parmak izlerini görmek için aşağıdaki adımları takip edin:

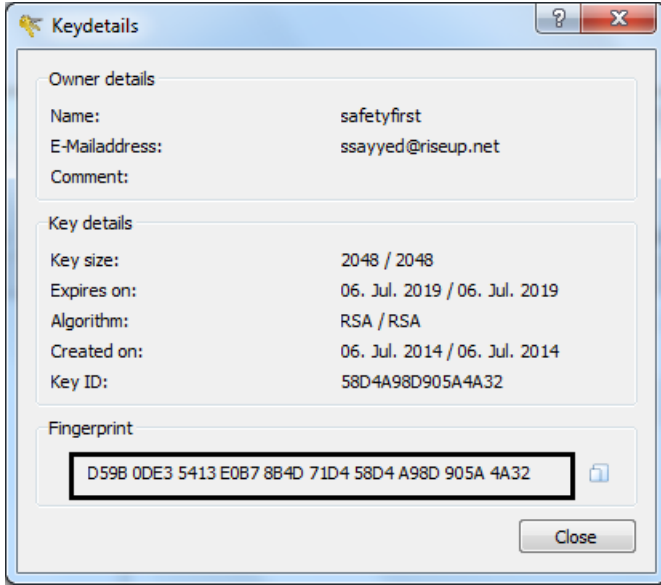
**1. Adım.** Bir anahtar **seçin**, aşağı açılır menüsünü etkinleştirmek için üzerine **sağ tıklayın**.

**2. Adım.** *Show Keydetails* (Anahtar detaylarını Göster) maddesini aşağıdaki Şekil 8'de görüldüğü gibi **seçin**.



Şekil 8: İletişim kuracağınız kişinin anahtarı ile ilişkili açılır menü

Bu şekilde aşağıdaki ekran etkinleşecektir:



Şekil 9: Aşağı bölümünde anahtar parmak izini gösteren Anahtar detayları penceresi

**3. Adım.** Bu parmak izini, iletişim kuracağınız kişinin kendi **gpg4usb** programında gördüğü ile **karşılaştırın**.

İletişim kuracağınız kişi de bu işlemleri gerçekleştirmelidir. Karşılıklı olarak gönderilen anahtarın gönderen kişinin orijinal anahtarı ile aynı olup olmadığından emin olun. Eğer aynı değilse yeniden açık anahtar paylaşımı yapın (farklı bir e-posta adresi veya iletişim yöntemi ile) ve doğrulama işlemlerini tekrarlayın.

Parmak izleri *tam* olarak örtüşüyorsa birbirinize güvenli ve şifreli mesaj ve dosyalar gönderebilir hale geldiniz demektir.

## Metin ve Dosyalar Nasıl Şifrelenir ve Deşifre Edilir?

Bu sayfadaki bölümlerin listesi:

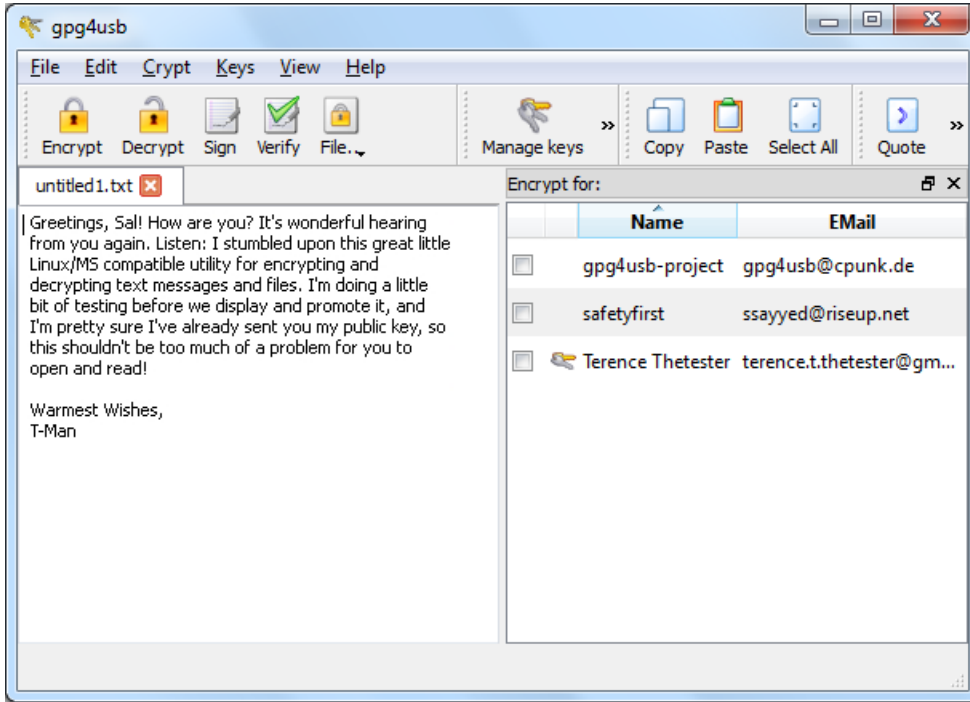
- **4.0 Yazılı İletiler gpg4usb Kullanarak Nasıl Şifrelenir**
- **4.1 Yazılı İletilerin Şifresi gpg4usb Kullanarak Nasıl Çözülür**
- **4.2 Dosyalar gpg4usb Kullanarak Nasıl Şifrelenir**
- **4.3 Dosyaların Şifresi gpg4usb Kullanarak Nasıl Çözülür**

### 4.0 Yazılı Mesajlar gpg4usb Kullanarak Nasıl Şifrelenir

Aşağıdaki örnekte Terence arkadaşı Salima'ya, aşağıdaki adımları takip ederek bir şifreli e-posta gönderecek:

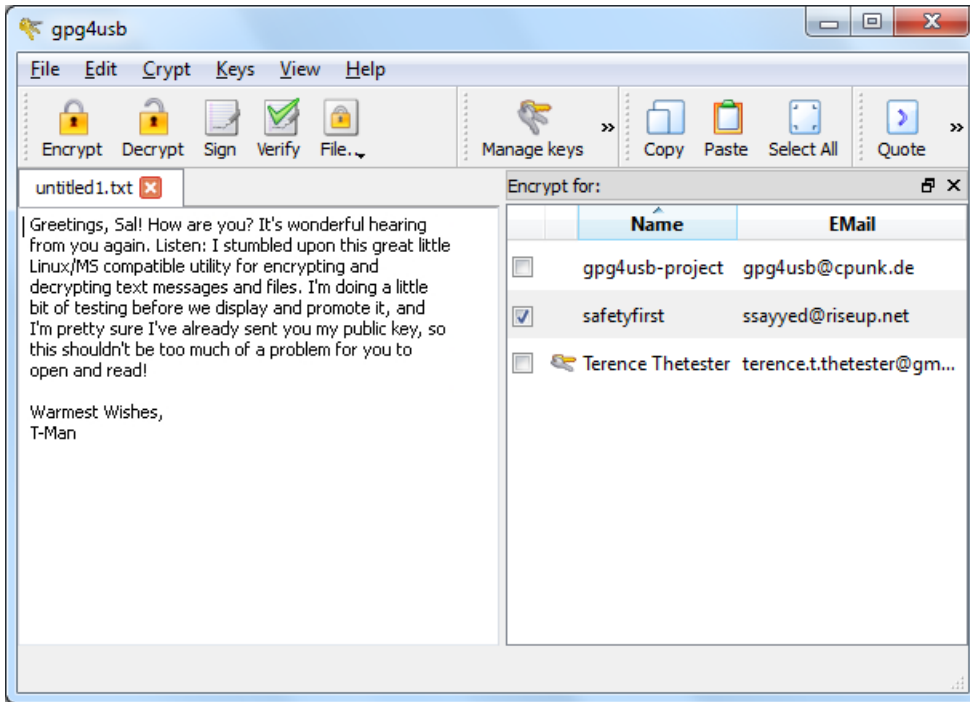
**1. Adım.** **gpg4usb** konsolunu açmak için  **start\_windows.exe**'ye **çift tıklayın**.

**2. Adım.** Mesajınızı aşağıdaki örnekte görüldüğü gibi **yazın**:



Şekil 1: Bir mesaj örneği gösteren gpg4usb konsolu

**3. Adım.** E-postayı göndereceğiniz kişi ile ilişkili kutuyu aşağıdaki gibi **seçin**:

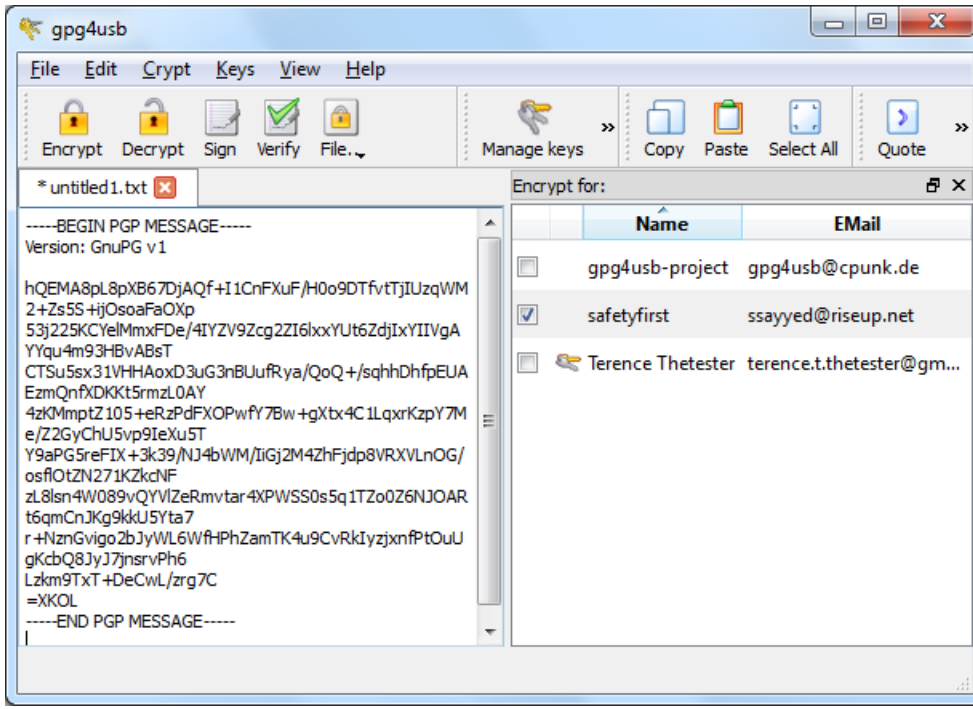


Şekil 2: E-posta gönderilecek kişiyi gösteren gpg4usb konsolu

**Not:** Bir iletiyi, *Encrypt for* (Bunlar için Şifrele) bölümünde bulunan ilgili kutuları tıklayarak birden fazla alıcı için şifreleyebilirsiniz. Kişisel kayıtlarınız için, iletiyi kendiniz için de şifrelemeyi faydalı bulabilirsiniz, çünkü, böylece iletiyi daha sonra kendiniz de okuyabilirsiniz.



**4. Adım.** **Encrypt** 'i tıklayarak yada **Crypt** (Şifreleme) menüsünden **select Encrypt**'i (Şifrelemeyi Seç'i) **tıklayarak** iletinizi aşağıdaki gibi şifreleyebilirsiniz:



Şekil 3: Şifrelenmiş bir ileti örneğini gösteren gpg4usb konsolu

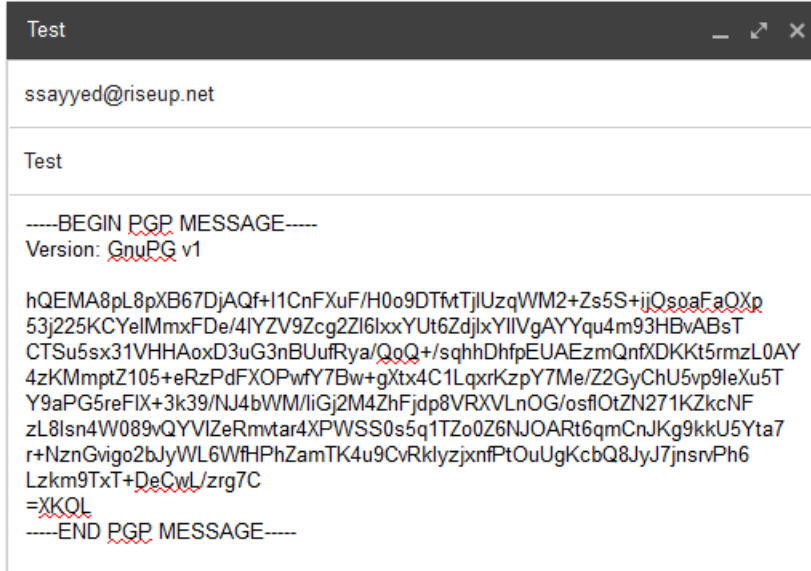


**5. Adım.** 'Select All' 'ı tıklayarak şifreli iletinin tümüyle seçin, ve 'Copy' 'yi tıklayarak iletiyi panoya kopyalayın.



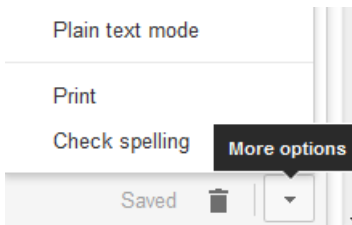
**Not:** Alternatif olarak, menüdeki her bir unsur ile ilişkili klavye kısa yollarını kullanabilirsiniz, bu durumda **Ctrl+E** iletiyi şifreler, **Ctrl+A** iletinin tümünü seçer, **Ctrl+C** iletiyi panoya kopyalar.

**6. Adım.** E-posta hesabınızı **açın** ve yeni bir ileti yazma penceresini **açın** sonrasında bu iletiyi aşağıdakine benzeyecek şekilde yapıştırın:



4. Şekil: gpg4usb'de şifrelenip Gmail hesabındaki bir e-postaya yapıştırılmış bir şifreli ileti örneği

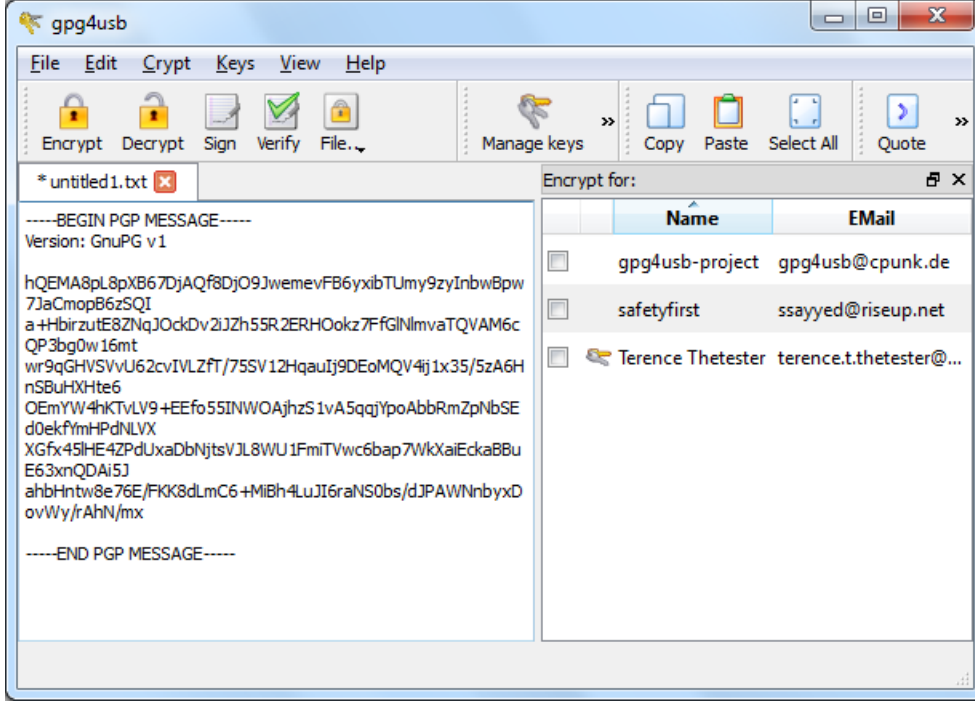
**Not: Rich Text Formats (RTF, Zengin Metin Formatları)** şifreli ileti formatını bozabilir; bu yüzden, iletilerinizi düz metinle yazmak daha iyidir. **Gmail'de RTF'yi** düz metne çevirmek için **Seçenekler'i** tıklayın, ve ileti bölümünün en altındaki **Düz metin mod'unu** seçin.



## 4.1 Yazılı İletilerin Şifresi gpg4usb Kullanarak Nasıl Çözülür

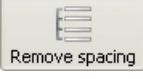
Şifrelenmiş bir e-postanın şifresini çözmek için aşağıdaki adımları takip edin:

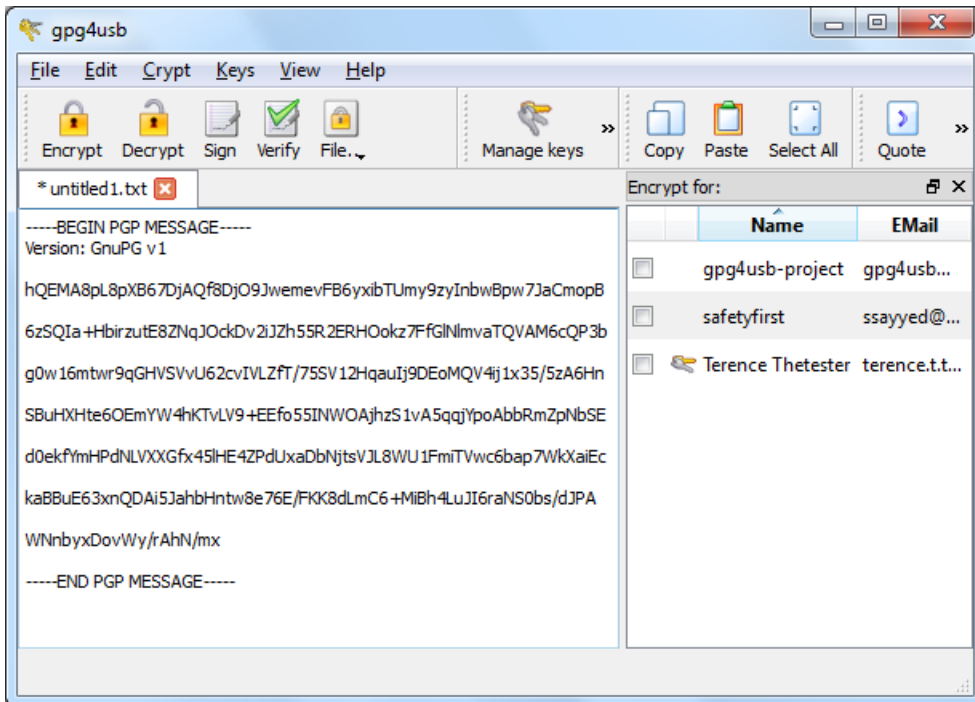
1. Adım. gpg4usb programını açmak için  start\_windows.exe'ye çift tıklayın.
2. Adım. E-posta hesabınızı ve iletiyi açın.
3. Adım. Şifrelenmiş mesajı seçin, kopyalayın ve gpg4usb konsolu untitled1.txt sekmesine aşağıdaki gibi yapıştırın:



Şekil 6: Şifresi çözülecek mesajı gösteren gpg4usb konsolu

**Not:** Şifreli metin, aşağıda Şekil 7'de görüldüğü gibi çift satır aralıkları ile görünüyorsa, gpg4usb otomatik olarak şifresini

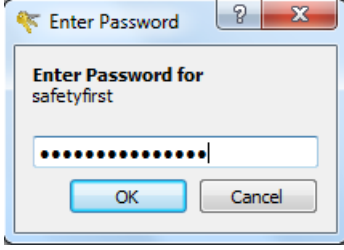
çözmeyebilir. Bu çift satır aralıklarını yok etmek için  Remove spacing'e tıklayın (ya da **Edit** [Düzenle] menüsünden *Remove double Linebreaks*'i [Çift Satır Aralıklarını Kaldır] seçin). Böylelikle, 4. Adım'da tarif edilen şifre çözme işlemine devam edebilirsiniz.



Şekil 7: Çift satır aralıklarına sahip şifresi çözülecek bir ileti gösteren gpg4usb konsolu



**4. Adım.** Decrypt'e tıklayın ve aşağıda görüldüğü gibi anahtar çifti oluştururken yarattığınız şifreyi girin.



Şekil 8: Şifre Gir uyarı penceresi

**5. Adım.** Yukarıdaki Şekil 2'de görüldüğü gibi **gpg4usb** konsolunu etkinleştirmek için **OK**'i (Tamam'ı) tıklayın.

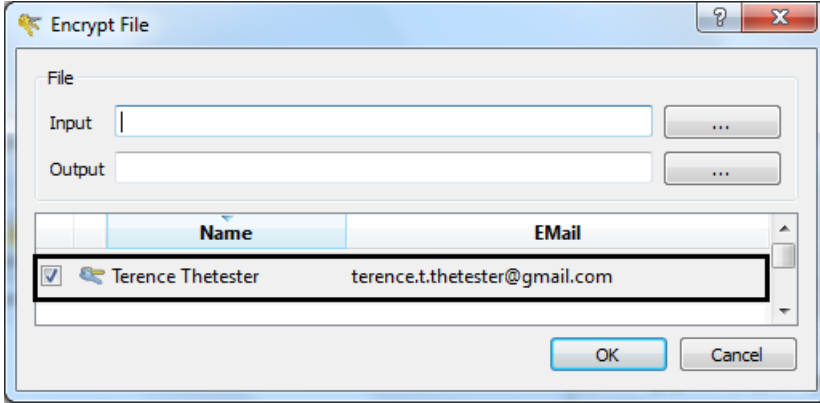
## 4.2 Dosyalar gpg4usb Kullanarak Nasıl Şifrelenir?

Bir dosyayı şifreleme işlemi yazılı iletileri şifrelemeye benzer. Aşağıdaki örnekte, Salima aşağıdaki adımları takip ederek Terence için bir dosyayı şifreleyecek.

**1.Adım.** **gpg4usb** programını açmak için start\_windows.exe'yi tıklayın.



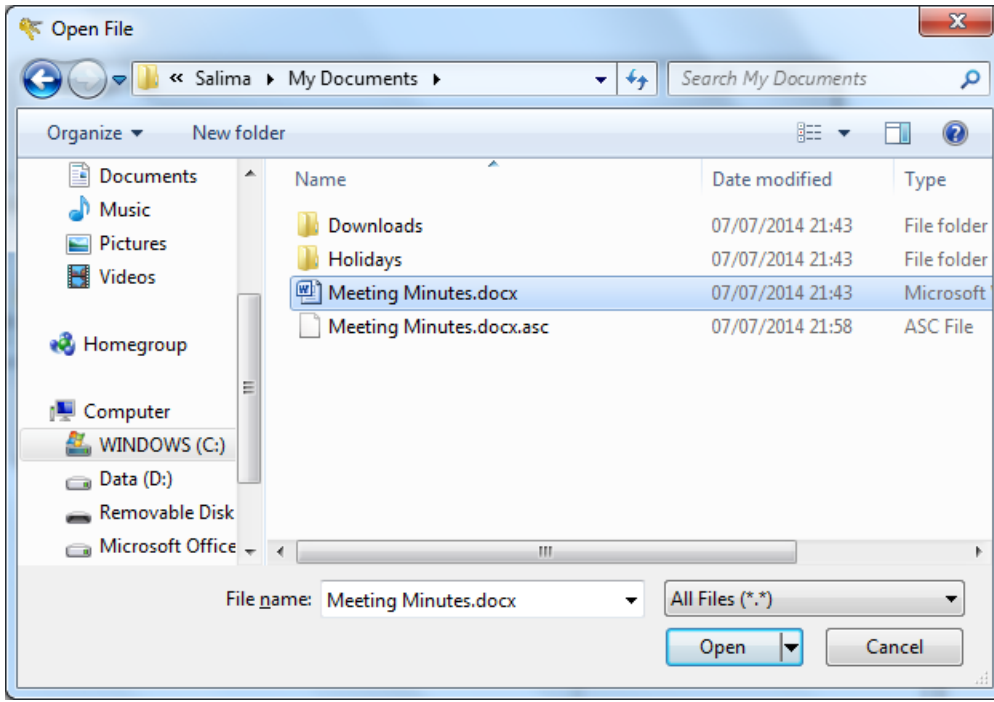
**2. Adım.** Aşağıdaki ekranı etkinleştirmek için File'ı ve **Encrypt File**'i (Dosyayı Şifrele'yi) tıklayın:



Şekil 9: Dosyayı Şifrele penceresi

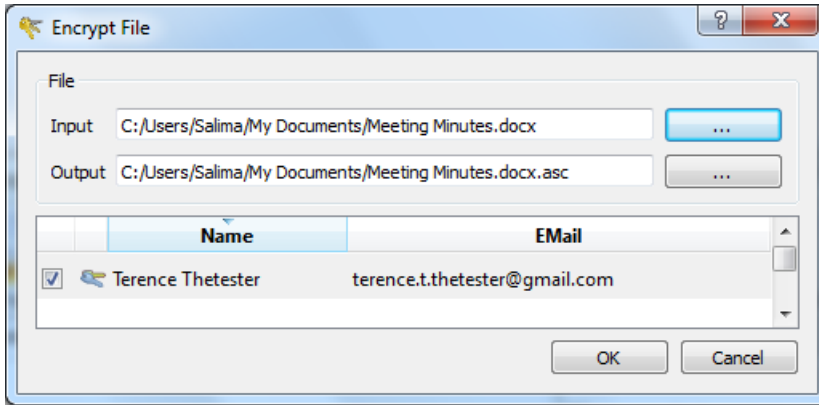
**Encrypt File** Dosyayı Şifrele penceresindeki kaydırma listesi (siyah ile gösterilmiş) iletinin şifrelenecek olan e-posta hesabını ve onunla bağlantılı anahtarı seçmenizi sağlar.

**3. Adım.** Aşağıdaki ekranı etkinleştirmek için **Input** (Girdi) maddesinin yanındaki ya tıklayın.



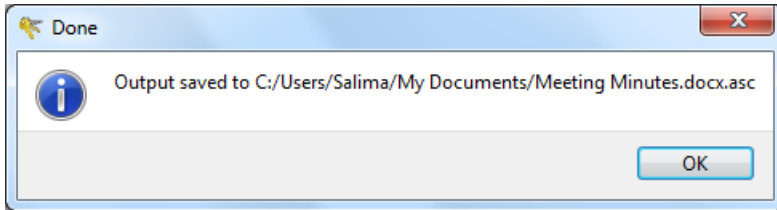
Şekil 10: Dosya Aç tarama penceresi

**4. Adım.** Şifrelenecek dosyayı eklemek için **Open** butonuna tıklayın ve *Encrypt* (Şifrele) ekranına aşağıda görüldüğü gibi dönün:



Şekil 11: Şifrelenecek olan dosyayı gösteren Dosya Şifrele penceresi

**5. Adım.** Aşağıdaki ekranı etkinleştirmek için **OK**'yi (Tamam'ı) tıklayın:



Şekil 12: Tamamlandı onaylama iletişim kutusu

*Tamamlandı* onaylama iletişim kutusu, yeni şifrelenmiş dosyaların nerede olduğunu gösterir. Şifrelenmiş bir dosya, .asc dosya uzantısı sayesinde de tanınabilir, örneğin, *Meeting Minutes.doc.asc*.

**6. Adım.** Dosya şifreleme işlemini tamamlamak için **OK**'i (Tamam'ı) tıklayın.

**Not:** Şifrelenmiş bir dosya ile göndereceğiniz iletiyi ayrıca şifreleyebilirsiniz.

**7. Adım.** E-posta hesabınızı kullanarak *Tamamlandı* onaylama iletişim kutusunda belirtilen yere **gidin** (Şekil 12) ve şifrelenmiş dosyayı herhangi bir dosya ekler gibi e-postanıza **ekleyin**.

**ÖNEMLİ:** Dosyanın adının **şifrelenmemiş** olduğuna dikkatinizi çekeriz. Bu adın hassas bilgiler içermediğinden emin olun! Ayrıca, aklınızda tutun ki bu dosyanın şifrelenmemiş bir versiyonu diskinizde yer almaya devam eder.

## 4.3 Dosyaların Şifresi gpg4usb Kullanarak Nasıl Çözülür

Aşağıdaki örnekte, Terence aşağıdaki adımları takip ederek Salima'nın ona gönderdiği dosyanın şifresini çözecek:

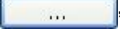
**1. Adım.** gpg4usb programını açmak için  start\_windows.exe'yi **çift tıklayın**.

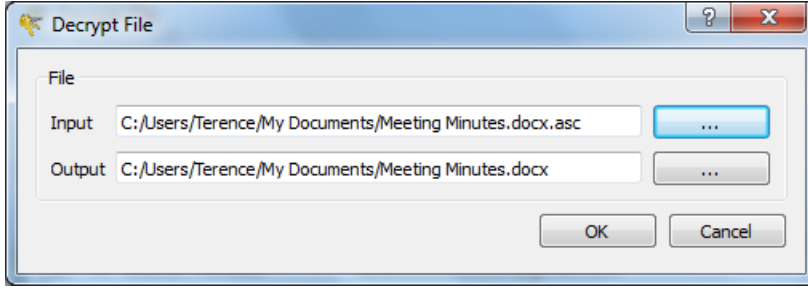
**2. Adım.** E-posta hesabınızı ve iletiyi **açın** ve eklenmiş dosyayı **indirin**.

**Not:** İletişim içinde olduğunuz kişi şifrelenmiş dosyayla birlikte bir mesaj da göndermişse, bu mesajı, **4.1. Yazılı İletilerin Şifresi gpg4usb Kullanarak Nasıl Çözülür?** <sup>[56]</sup> bölümünde anlatılan yöntemi kullanarak çözebilirsiniz.



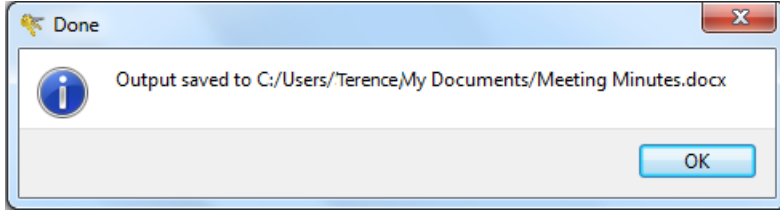
**3. Adım.** gpg4usb konsolunda (yukarıdaki Şekil 1'de gösterildiği gibi), File... 'a ve **Decrypt File** (Dosyanın Şifresini Çöz) penceresine **tıklayın** (aşağıdaki Şekil 13'te görüldüğü gibi).

**4. Adım.** İndirilen şifrelenmiş dosyayı bulmak için aşağıda görüldüğü gibi *Input* (Girdi) maddesinin yanındaki  'ya **tıklayın**.



Şekil 13: Şifrelenmiş dosyaya giden yolu gösteren Şifre Çöz penceresi

**5. Adım.** Aşağıdaki ekranı etkinleştirmek için **OK**'yi (Tamam'ı) **tıklayın**:



Şekil 14: Şifresi çözülmüş dosyanın yerini gösteren Tamamlandı onaylama iletişim kutusu

**Önemli:** Bir internet kafede veya iş yerinde çalışıyorsanız, diğer kişilerin şifresi çözülmüş dosyaya erişimi olabilir. .asc uzantısına sahip dosyayı USB veya taşınabilir sürücüyü kopyalamak ve evinize götürüp şifre çözme işlemini orada güvenli bir şekilde yapmak daha iyidir.

## Sıkça Sorulan Sorular ve Gözden Geçirme

### 5.0 Sıkça Sorulan Sorular

**Soru:** gpg4usb, sadece USB çubuğunda mı kullanılabilir?

**Cevap:** Hayır. Bilgisayarınızın sabit diskine çıkartılıp oradan da çalıştırılabilir.

**Soru:** Kaç hesap için anahtar çifti oluşturabilirim?

**Cevap:** Ne kadar isterseniz.

**Soru:** Basit kopyalama ve yapıştırma işlemleri kullanılması oldukça güzel.

**Cevap:** Gerçekten de öyle. Fakat unutmayın ki e-posta konu kutusunda yazılanlar şifrelenmemiş bir şekilde kalır. Bu yüzden, dikkatli olun ve e-posta içeriği veya sizi ele verecek bir şey yazmayın!

### 5.1 Gözden Geçirme Soruları

- Açık anahtarı imzalamak ve doğrulamak arasındaki fark nedir?
- Parmak izi nedir ve nasıl kullanılır?

# CCleaner – Güvenli Dosya Silme ve Çalışma Oturumu Temizleme

## Short Description:

**CCleaner**, dijital gizliliğiniz ve güvenliğini korumak için vazgeçilemez, kullanımı kolay ve verimli bir programdır. **CCleaner**, tarama geçmişinizi, çalışma oturumunuz esnasında oluşturulmuş geçici dosyaları ve boş disk alanınızı silerek (veya ortadan kaldırarak), kötü amaçlı ve zararlı kişilerin sisteminizi tehlike altına sokmasını veya çalışma alışkanlık ve tercihlerinizi izlemelerini engeller.

## Online Installation Instructions:

### CCleaner'ı Kurma

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **CCleaner** ikonunu **tıklayarak** [www.piriform.com/ccleaner/builds](http://www.piriform.com/ccleaner/builds) sayfasını açın
- **-CCleaner – Slim** bölümündeki **'İndir'** tuşuna **basın**
- **'ccsetup\_slim.exe'**yi bilgisayarınıza **kaydedin** ve programı kurmayı başlatmak için üzerine **çift tıklayın**
- Devam etmeden önce bir sonraki bölümdeki **'kurulum talimatları'**nı okuyun
- **CCleaner**'ı başarılı bir şekilde indirdikten sonra programı bilgisayarınızdan silebilirsiniz

### CCleaner:



[57]

### Ana Sayfa

[www.ccleaner.com](http://www.ccleaner.com) <sup>[58]</sup>

### Bilgisayar Gereksinimleri

- Tüm Windows Sürümleri

### Bu Rehberde Kullanılan Sürüm

- 5.06

### Lisans

- Ücretsiz Yazılım

### Bu bölümün güncellendiği tarih

- Ağustos 2014

### Gerekli Okumalar

Nasıl Yapmalı kitapçığı, **6. Hassas bilgiler nasıl imha edilir** <sup>[59]</sup> bölümü

### Buradan sağlayacağınız faydalar:

- Etkinliklerinizin ve bilgisayarınıza geçici olarak kaydedilmiş belgelerin izlerini kalıcı olarak silebilmek
- Bilgisayarınıza bağlı disklerdeki boş alanları temizleyebilmek
- Windows Kayıt Defterini temizleyebilmek
- Bilgisayarınız başladığında hangi programların açılacağını kontrol edebilmek

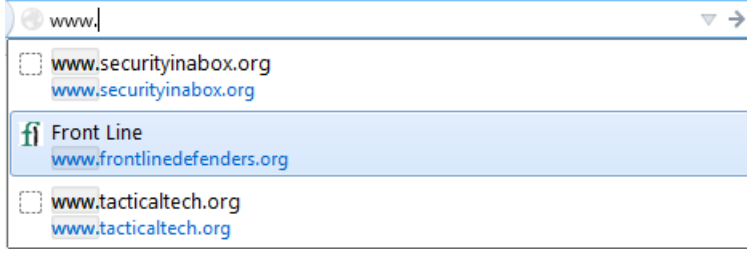
### GNU Linux, Mac OS ve Microsoft Windows ile çalışan diğer programlar

**GNU Linux** ve **Microsoft Windows** ile uyumlu başka bir geçici dosya silici ve yok edici program, **BleachBit**'tir <sup>[60]</sup>. **BleachBit**, 70 popüler uygulamanın geçici dosyalarını, işletim sisteminizin geçici dosyalarını ve hard diskinizdeki geçici dosyaları silmenize olanak verir. Taşınabilir versiyonu bulunan bir açık kaynak program olan **BleachBit**, 32 dilde kullanıma hazırdır.

**CCleaner**'in **Mac OS** ile uyumlu bir versiyonu da bulunur. Fakat kullanıcılar, çalışma oturumlarının izlerini silmek için **Titanium's Software**'den, **OnyX** ve **Maintenance**](<http://www.titanium.free.fr/>) gibi ücretsiz araçları da tercih edebilirler. **Çöp Kutunuzu** güvenli bir şekilde temizlemek için, **Bul** menüsünü açın ve **Bul > Çöp Kutusunu güvenli boşalt**'ı **seçin**. **Çöp kutunuzu** her zaman güvenli bir şekilde boşaltmak için, **Bul > Tercihler**'i **seçin** ve **Gelişmiş** sekmesine **tıklayın**. **Çöp kutusunu güvenli boşalt** seçeneğini seçin. Diskteki boş bölümü temizlemek için, **Disk Yardımcı Programı** sistem uygulamasını **çalıştırın**, disk bölmesini **seçin**, **Sil** sekmesini **seçin** ve **Boş Alanı Sil** düğmesine **tıklayın**.

## 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

Bilgisayar sisteminizde veya bir İnternet tarayıcısındaki verili ayarlar, otomatik olarak, bu konuda bilgili olan ve kötü amaçlı tarafların takip edebileceği bir veri izi yaratır. Her İnternet tarayıcısı veya sözcük işlemcisi veya programı kullandığınızda, bilgisayar sisteminize geçici veriler ve dosyalar kaydeder. En son görülmüş belge ve web sayfalarının listesini de oluşturabilir. Örneğin, İnternet tarayıcınıza herhangi bir web adresi yazdığınız zaman, o harflerle başlayan diğer adreslerin listesini, aşağıda görüldüğü gibi gösterir:



Şekil 1: Farklı URL'leri gösteren bir İnternet tarayıcısı adres çubuğu

Tarama geçmişleri bazı durumlarda işe yarasa da, gezmiş olduğunuz web sitelerinin tespit edilmesine neden olabilir. Ayrıca, bu web sitelerinde görünen imajlar veya e-posta adresleri ve İnternet forumlarına girilmiş olan bilgiler aracılığıyla, aktivitelerinizin tespit edilmesine yarayabilecek geçici bir veri tabanı oluşturur.

Bir programı her kullandığınızda oluşan geçici verileri ortadan kaldırmak için, ger programın kendi dizinini açmanız ve program dosyalarını manuel olarak seçip silmeniz gerekir. **CCleaner** size bu programların listesini sunar ve silmek istediğiniz geçici dosyalara sahip olan programları seçmenizi sağlar.

**Önemli:** **CCleaner**, bilgisayarınıza kaydedilmiş gerçek dosyalara dokunmadan sadece geçici dosyaları siler fakat yine de belgelerinizin düzenli olarak yedeklemenizi **şiddetle tavsiye ederiz** (yedekleme konusunda daha fazla bilgi için lütfen Nasıl Yapmalı kitapçığı'nın, **5. Veri kayıpları nasıl kurtarılır** <sup>[61]</sup> bölümüne bakın).

**CCleaner**'ı çalıştırdıktan sonra tüm tarayıcı ve yakın tarihli belge geçmişinizi kaybedebilirsiniz. Bu da bu programın amacıdır, bu program bilgisayar sisteminizin maruz kaldığı virüs ve kontrol mekanizmalarını minimuma indirir.

### Offline Installation Instructions :

#### CCleaner Kurma

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **CCleaner** ikonunu **tıklayın** ve yükleyiciyi 'Aç'ın veya 'Çalıştır'ın. Gerekirse yükleyiciyi önce kaydedin, daha sonra üzerine çift tıklayın
- Devam etmeden önce bir sonraki bölümdeki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulum bittikten sonra silebilirsiniz

#### CCleaner:



[62]

## CCleaner Nasıl Kurulur ve Yapılandırılır

List of sections on this page:

- **2.0 CCleaner Nasıl Kurulur**
- **2.1 CCleaner'ı Yapılandırmaya Başlamadan Önce**
- **2.2 CCleaner Nasıl Yapılandırılır**

### 2.0 CCleaner Nasıl Kurulur

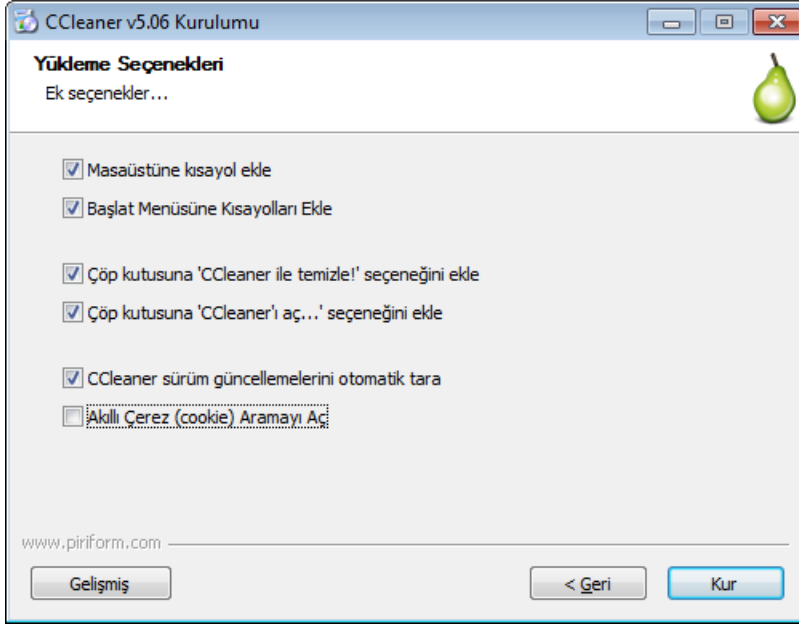
**CCleaner** kurmak görece olarak kolay ve hızlı bir işlemdir. **CCleaner**'ı kurmaya başlamak için aşağıdaki adımları takip edin:

**1. Adım.** Kurulum işlemini başlatmak için  'e **çift tıklayın**. Uyarı iletişim kutusu açılabilir. Açılırsa **Evet'i** **tıklayın** ve aşağıdaki ekranı etkinleştirin:



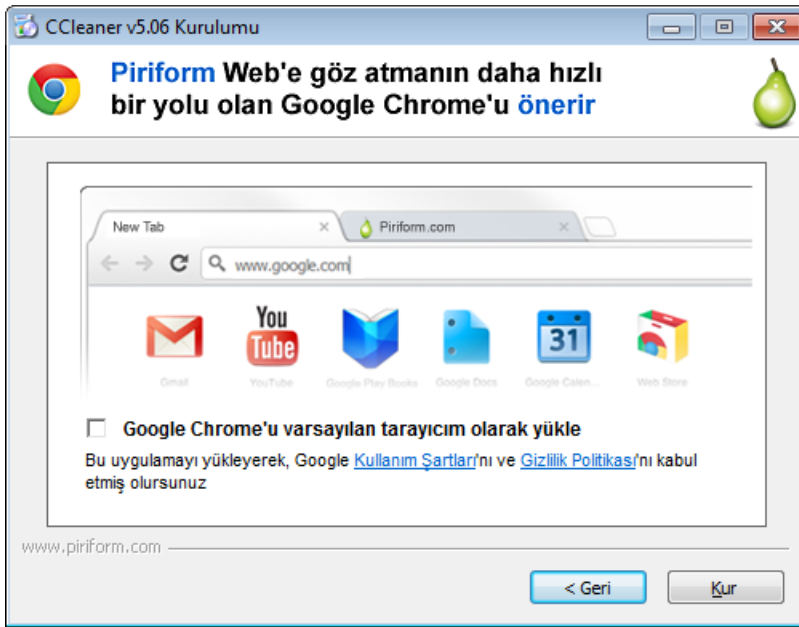
Şekil 1: CCleaner v5.06 Kurulum Sihirbazına Hoş Geldiniz penceresi

**2. Adım.** Aşağı Açılır Menü'den Türkçe'yi kurulum dili olarak seçin *Yükleme Seçenekleri – Ek seçenekler...* penceresini etkinleştirmek için **Next >** 'i tıklayın.



Şekil 2: Yükleme Seçenekleri – Ek Seçenekler... penceresi

**3.Adım:** *Yükleme Seçenekleri – Ek seçenekler...* penceresinde \*Akıllı Çerez (cookie) aramayı geç seçeneğinin işaretini yukarıdaki gibi kaldırın ve aşağıdaki ekranı etkinleştirmek için **İleri >** 'yi ya da **Kur** 'u tıklayın:

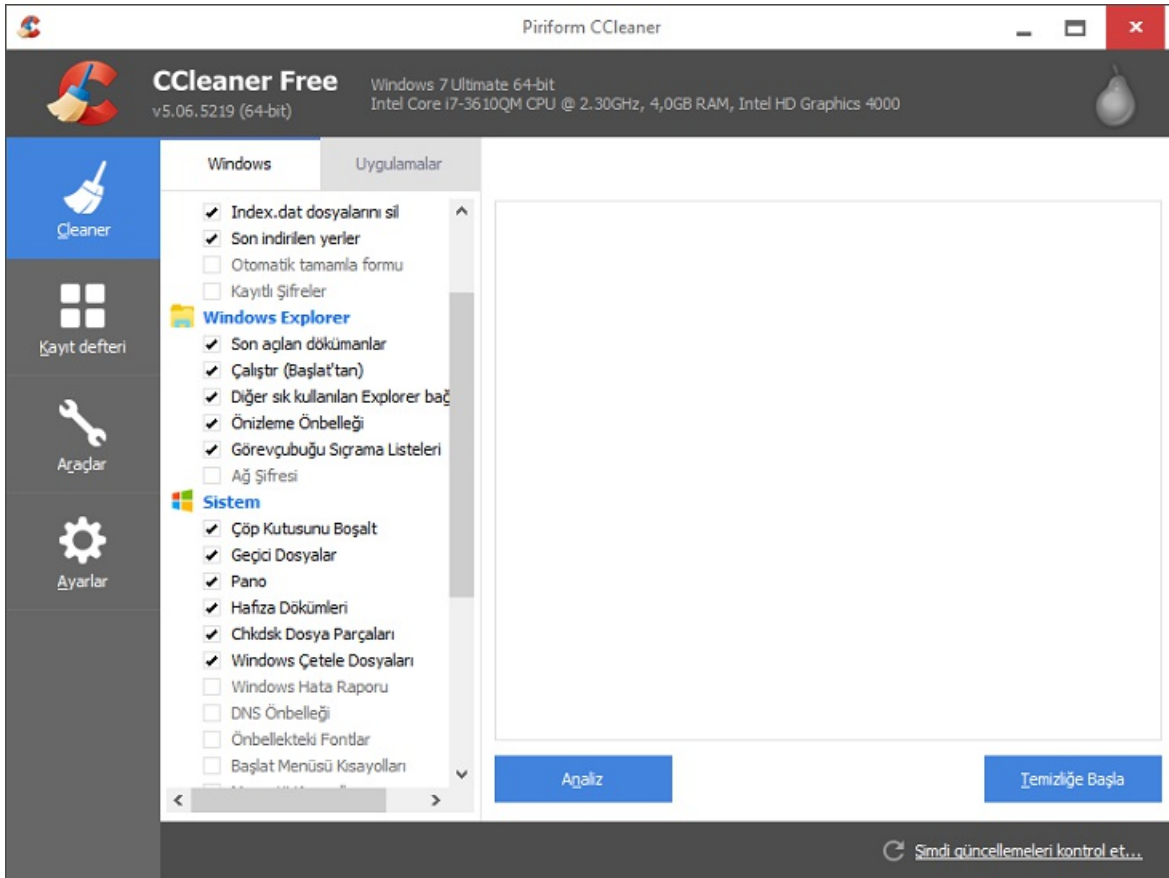


Şekil 3: Google Chrome'u verili tarayıcı penceresi olarak kur

**3. Adım.** Google Chrome'u verili tarayıcı penceresi olarak kur seçeneğini, yukarıdaki Şekil 2'de görüldüğü gibi etkisizleştirin. Bu sayede Google Chrome'un kendisini bilgisayarınıza otomatik olarak kurmasını engellemiş olursunuz. Bu ekran görünmeyebilir de.

**4. Adım.** Kurulum gelişim statü çubuğunu gösteren Kurulum ekranını etkinleştirmek için **Kur** butonuna tıklayın.

**5. Adım.** CCleaner kurulumunu bitirmek için **Bitir** butonuna tıklayın ve CCleaner ana konsolunu açın.



Şekil 4: Piriform CCleaner ana konsolu

## 2.1 CCleaner'ı Yapılandırmaya Başlamadan Önce

**Nasıl Yapmalı Kitapçığı 6. Hassas bilgiler nasıl imha edilir** [59] Bölümü'nde detaylı bir şekilde anlatıldığı gibi, Microsoft Windows standart dosya silme yöntemleri, diskinizdeki temel verileri silmez (Geri Dönüşüm Kutusunu boşaltsanız bile). Bu geçici dosyalar için de geçerlidir. Onları sabit diskinizden kalıcı olarak silmek için (ya da ortadan kaldırmak için),

dosyaların üzerine rastgele verilerin yazılması gerekir. **CCleaner**, silinen dosyaların güvenli bir şekilde silinmesi için onların üzerine yazacak şekilde yapılandırılmalıdır, çünkü verili modunda bunu yapmaz. **CCleaner** aynı zamanda, diskin boş alanlarını temizleyerek eskiden silinmiş dosyaları da temizleyebilir (bunun için lütfen **5.3 CCleaner Kullanarak Boş Alan Nasıl Temizlenir** bölümüne bakın).

## 2.2 CCleaner Nasıl Yapılandırılır

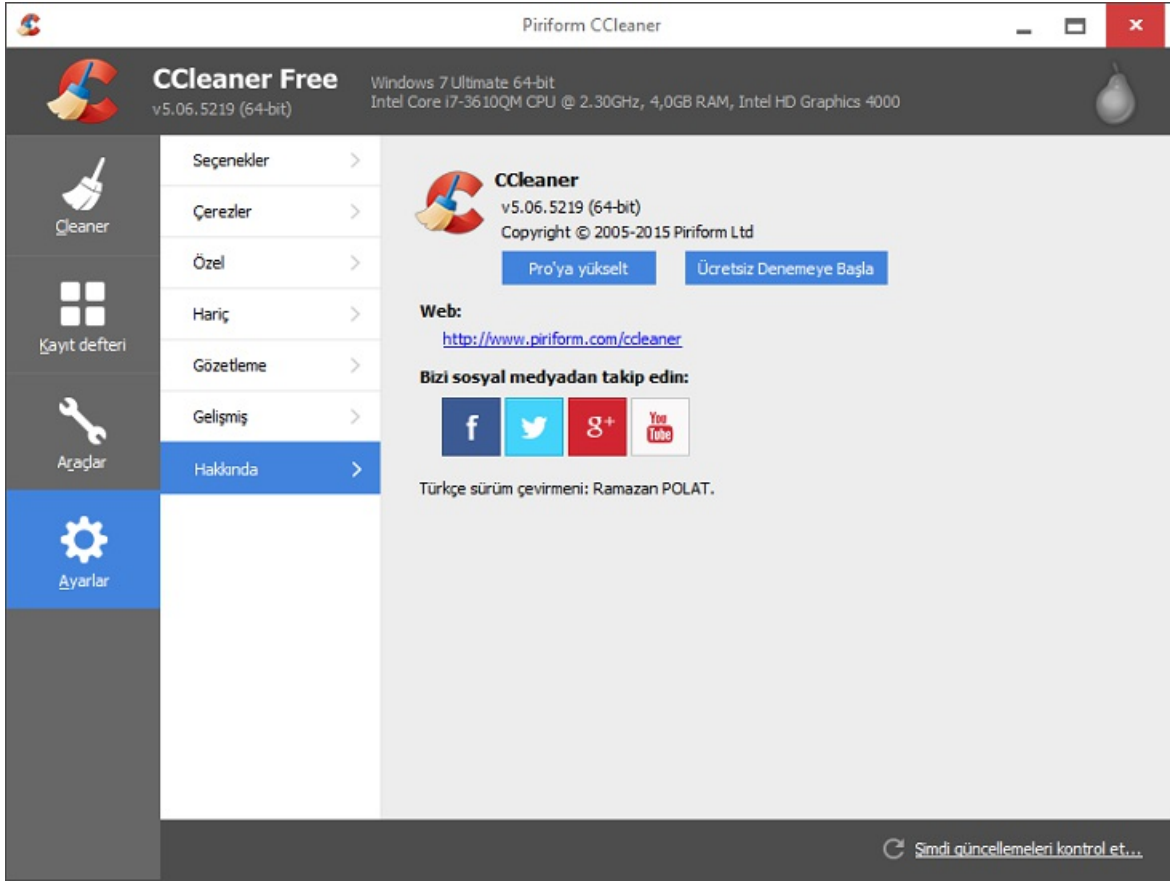
**CCleaner** kullanılmaya başlamadan önce, tüm geçici dosyaları güvenli silecek şekilde yapılandırılmalıdır.

**CCleaner**'i yapılandırmak için aşağıdaki adımları takip ediniz:

1. **Adım.** *Piriform CCleaner* konsolunu etkinleştirmek için 'e **tıklayın** ya da **Başlat > Programlar > CCleaner**'i seçin.



2. **Adım.** Aşağıdaki ekranı etkinleştirmek için 'ı **tıklayın**.



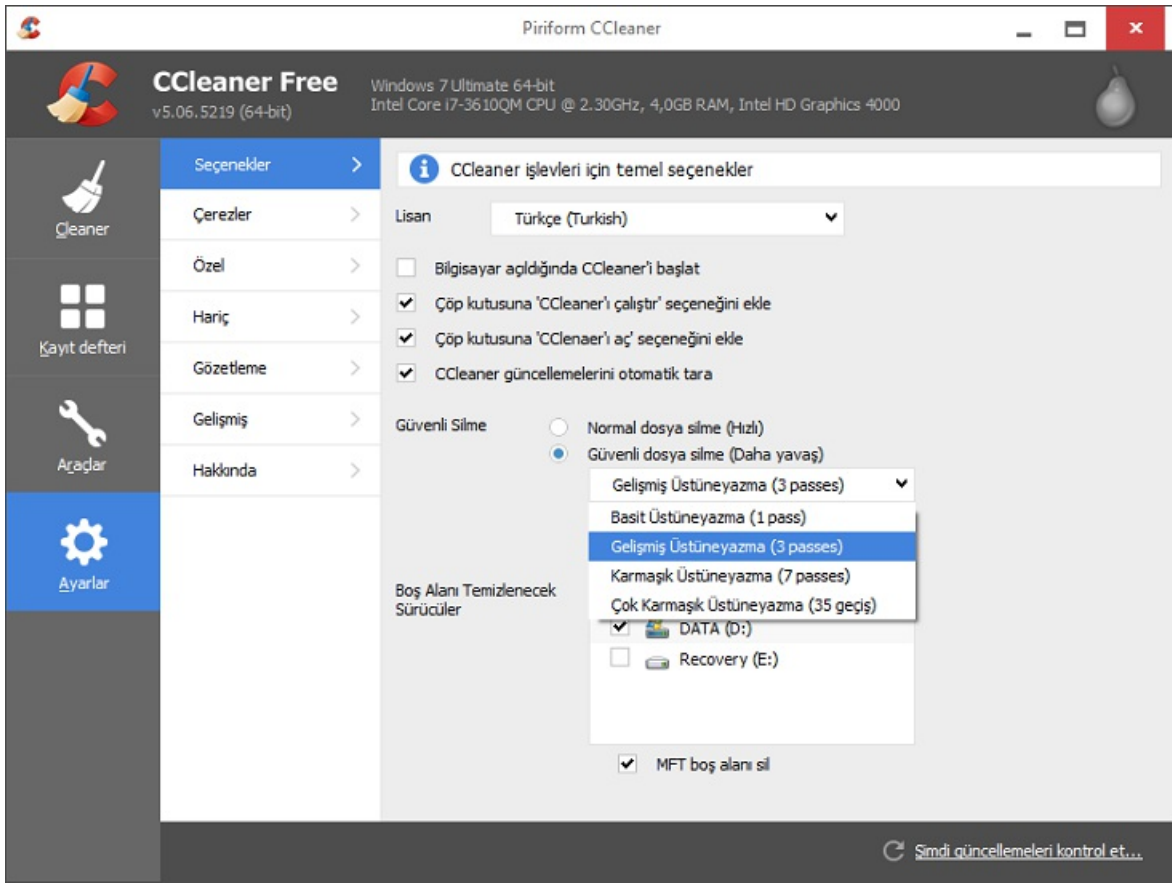
Şekil 6: Verili Hakkında sekmesini gösteren Seçenekler penceresi

3. **Adım.** *Ayarlar* sekmesini etkinleştirmek için 'i **tıklayın**. *Ayarlar* sekmesinde istediğiniz dili seçebilirsiniz ve **CCleaner**'in geçici dosyaları nasıl sileceğini ve diskleri nasıl temizleyeceğini seçebilirsiniz.

**Not:** *Güvenli Dosya Silme* bölümü, *Normal dosya silme* seçeneği seçili olarak belirir.

4. **Adım.** Aşağı açılır listeyi etkinleştirmek için *Güvenli dosya silme (yavaş)* seçeneğini **tıklayın**.

5. **Adım.** *Güvenli dosya silme (yavaş)* aşağı açılır menüsünü **tıklayın** ve aşağıdaki ekranı etkinleştirmek için *Gelişmiş Üstüneyazma (3 passes)* seçeneğini **seçin**.



Şekil 5: Güvenli Silme seçeneklerini gösteren Ayarlar sekmesi

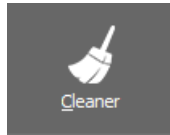
Bu ayarı yaptıktan sonra, **CCleaner**, rastgele verilerle silmeyi seçtiğiniz dosya ve klasörlerin üzerine yazacak ve onları sabit diskinizden etkin bir şekilde silecektir. Güvenli sil aşağı açılır menüsündeki 'kere' seçeneği, sileceğiniz dosyaların üzerine kaç kere rastgele veri yazılacağını belirler. Bu sayıyı ne kadar artırırsanız, silinecek olan dosya veya klasörlerinizin üzerine o kadar çok rastgele veri yazılacaktır. Bu durum dosya, belge veya klasörlerinizi geri getirmenizi zorlaştırır ama silme işleminin süresini de uzatır.

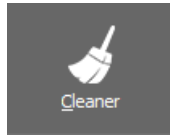
## CCleaner ile Geçici Dosyalar Nasıl Silinir

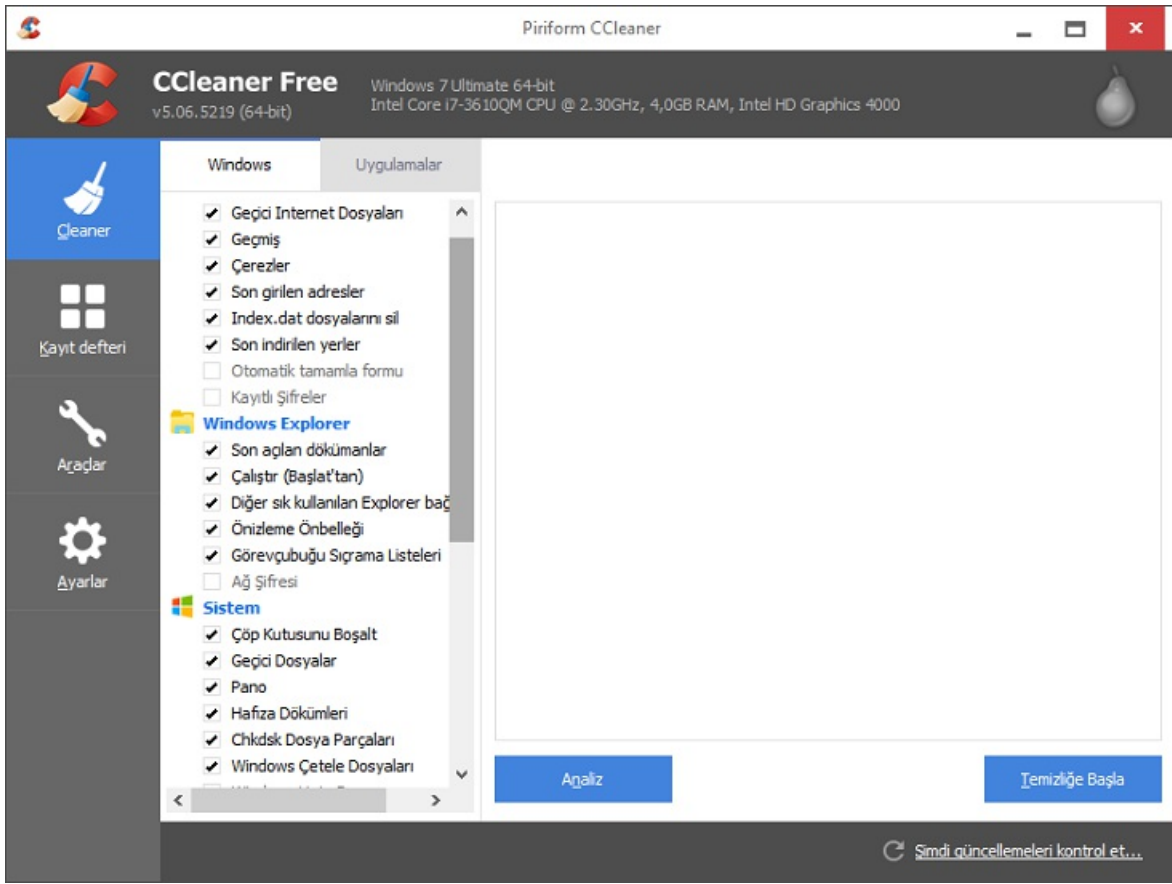
### 3.0 Geçici Dosyalar Nasıl Silinir

Bu bölümde, **Microsoft Windows** ve bilgisayarınızda kullandığınız diğer uygulamaların oluşturduğu dosyaları nasıl sileceğinizi anlatacağız.

1. Adım. **CCleaner** konsolunu etkinleştirmek için 'e **tıklayın** veya **Başlat >Programlar > Ccleaner'ı seçin**.

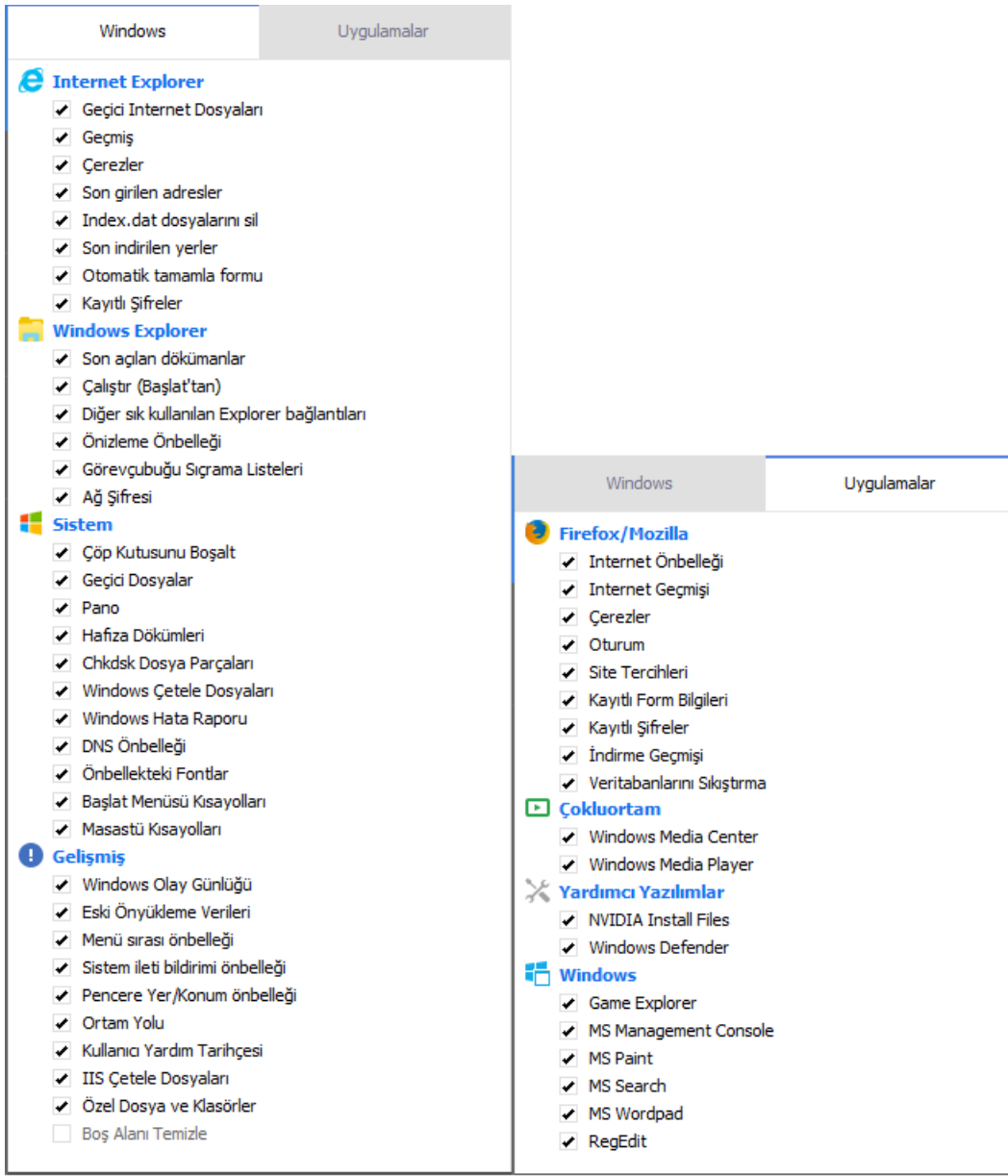


2. Adım. Aşağıdaki ekranı etkinleştirmek için 'e **tıklayın**:



Şekil 1: Cleaner sekmesini gösteren CCleaner konsolu

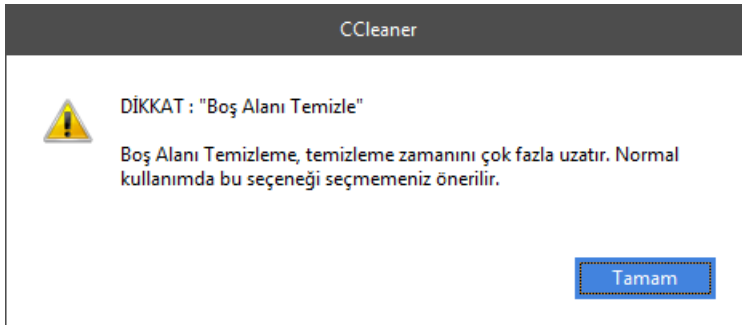
Cleaner penceresi iki bölme ayrılmıştır. Soldaki bölme Windows ve Uygulamalar sekmelerini gösterirken, sağdaki bölme temizleme işlemi ile ilgili bilgileri ve bu işlemin sonuçlarını gösterir. Bu bölümün altında, Analiz ve Temizliğe Başla düğmeleri yer alır.



Şekil 2: Tüm seçenekler işaretlenmiş Windows ve Uygulamalar sekmeleri

**Not:** Aşağıdaki adımları takip ederek, *Windows* ve *Uygulamalar* sekmelerinde seçmiş olduğunuz tüm geçici dosyaları sileceksiniz. Farklı kullanıcıların bilgisayarlarında farklı programlar olduğunu göz önünde bulundurursak, uygulamalar listenizin *Şekil 2'de* görünenden farklı olacağını göz önünde bulundurun.

**3. Adım.** *Windows* ve *Uygulamalar* sekmelerinde **asağı kaydırın** ve *Gelişmiş* bölümündeki tüm seçenekleri de **işaretleyin**. Bu seçenekleri işaretlerken, bir uyarı iletişim kutusu ile karşılaşabilirsiniz. Bu kutu her seçeneğin neleri etkileyeceğini gösterir.



Şekil 3: Uyarı onay iletişim kutusu örneği

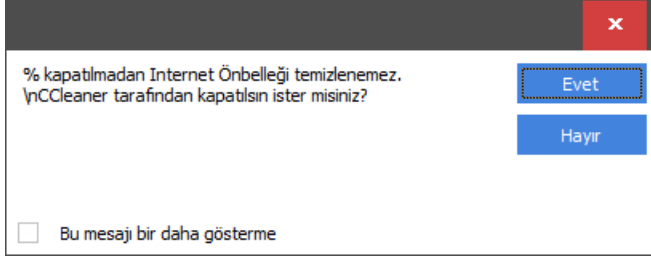
**Uyarı:** Boş Alanları Temizle seçeneğini işaretlerseniz, temizleme işleminin süresini bir hayli uzatırsınız. Bunu yapmadan önce, en az 1 ya da 2 saatiniz olduğundan emin olun.

**Not:** Geçici dosyaları etkin bir şekilde temizleyebilmek için *Windows* ve *Uygulamalar* sekmelerindeki tüm seçenekleri **işaretleyin**. Fakat, hangi yapılandırmaların ve ayarların silindiğini anladığınızdan emin olmalısınız. Her mesajı kapatmak

ve geçici dosya silme işlemine devam etmek için **Tamam** 'ı tıklayın.

**4. Adım.** Silinmek için hazır olan farklı geçici dosyaların listesini görmek için **Analiz** 'i tıklayın.

**İpucu:** Temizleme işlemine başlamadan önce tüm diğer programları kapatın. Herhangi başka bir programı açık bırakırsanız, **CCleaner** bu programlarla bağlantılı olan geçici dosyaları silmeyebilir ve aşağıdaki *Şekil 4*'e benzer bir uyarı ile karşılaşabilirsiniz.



*Şekil 4: Bir programı kapatma uyarısı örneği*

**5. Adım.** Silinecek dosyaları listelemeye devam etmek için **Evet** 'i tıklayın.

100%

**Analiz bitti! - (0.401 saniye)**  
358 MB silinecek. (Yaklaşık boyut)  
Güvenli Dosya Silme Aktifleştirildi - Gelişmiş Üstüneyazma (3 passes)

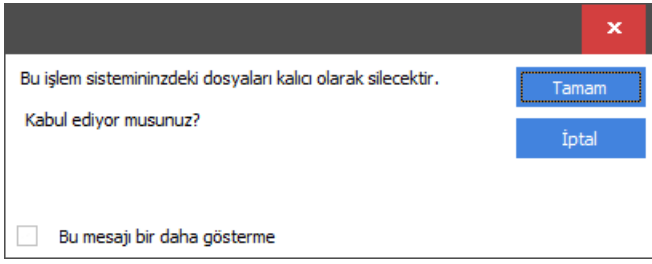
**Silinecek dosyaların detayı (Not: Henüz dosyalar silinmedi)**

|  |                                               |            |             |
|--|-----------------------------------------------|------------|-------------|
|  | Internet Explorer - Geçici Internet Dosyaları | 14.871 KB  | 431 dosya   |
|  | Internet Explorer - Geçmiş                    | 300 KB     | 10 dosya    |
|  | Internet Explorer - Çerezler                  | 564 KB     | 35 dosya    |
|  | Internet Explorer - Index.dat dosyalarını sil | 592 KB     | 4 dosya     |
|  | Windows Explorer - Son açılan dokümanlar      | 69 KB      | 29 dosya    |
|  | Sistem - Çöp Kutusunu Boşalt                  | 2.710 KB   | 2 dosya     |
|  | Sistem - Geçici Dosyalar                      | 307.049 KB | 460 dosya   |
|  | Sistem - Windows Çetele Dosyaları             | 9.487 KB   | 27 dosya    |
|  | Sistem - Windows Hata Raporu                  | 860 KB     | 48 dosya    |
|  | Sistem - Önbellekteki Fontlar                 | 10.282 KB  | 5 dosya     |
|  | Gelişmiş - IIS Çetele Dosyaları               | 41 KB      | 9 dosya     |
|  | Firefox/Mozilla - Internet Önbelleği          | 17.865 KB  | 1.297 dosya |
|  | Firefox/Mozilla - Internet Geçmişi            | 409 KB     | 10 dosya    |
|  | Firefox/Mozilla - Çerezler                    | 0 KB       | 62 dosya    |
|  | Firefox/Mozilla - Oturum                      | 13 KB      | 3 dosya     |
|  | Firefox/Mozilla - Site Tercihleri             | 288 KB     | 2 dosya     |
|  | Firefox/Mozilla - Kayıtlı Form Bilgileri      | 192 KB     | 1 dosya     |
|  | Windows - MS Search                           | 1.024 KB   | 1 dosya     |

*Şekil 5: Silinecek geçici dosyalar listesi örneği*

**Not:** **CCleaner**, sadece bir uygulama kullandığınız zaman oluşmuş olan geçici dosyaları siler. Uygulamanın kendisini silmez. Örneğin, *Şekil 5*'te, *Uygulamalar – Internet Explorer* programı bilgisayarınızda kurulu kalırken, onun geçici dosyaları silinir. **CCleaner**'ı bir programı kaldırmak için kullanmak isterseniz, **Sıkça Sorulan Sorular ve Gözden Geçirme bölümünde** <sup>[63]</sup>, Gelişmiş Seçenekler kısmında, **5.1 CCleaner Kullanarak Nasıl Programlar Devre Dışı Bırakılır**'a bakabilirsiniz.

**6. Adım.** Aşağıdaki ekranı etkinleştirmek için **Temizliğe Başla** 'yı tıklayın:



Şekil 6: Kalıcı dosya silme onayı uyarısı

**7. Adım.** Bu geçici dosyaları silmek için **Tamam** butonuna tıklayın. Silme işlemi tamamlandıktan sonra, sonuçlar aşağıdaki ekrandaki gibi görünecektir:



Şekil 7: Silme sonuçları

Geçici dosyalarınızı **CCleaner** kullanarak *Windows* ve *Uygulamalar* sekmelerinden başarı ile sildiniz. .

## Windows Kayıt Defteri CCleaner Kullanarak Nasıl Temizlenir

List of sections on this page:

- [4.0 Başlamadan Önce](#)
- [4.1 Windows Kayıt Defteri CCleaner Kullanarak Nasıl Temizlenir](#)
- [4.2 2 Kayıt Defteri Yedekleme Dosyası Nasıl Geri Kazanılır?](#)

### 4.0 Başlamadan Önce

**CCleaner**, sisteminizde yapılandırma bilgilerini, donanım ve yazılım ayarlarınızı saklayan bir veri tabanı oluşturan **Windows Kayıt Defteri**'ni temizlemenize olanak sağlar. Sistem yapılandırma bilgilerinizi değiştirdiğiniz, yazılım indirdiğiniz veya başka rutin işlemler yaptığınız zaman, bu değişiklikleri **Windows Kayıt Defteri**'nde belirir ve kaydedilir.

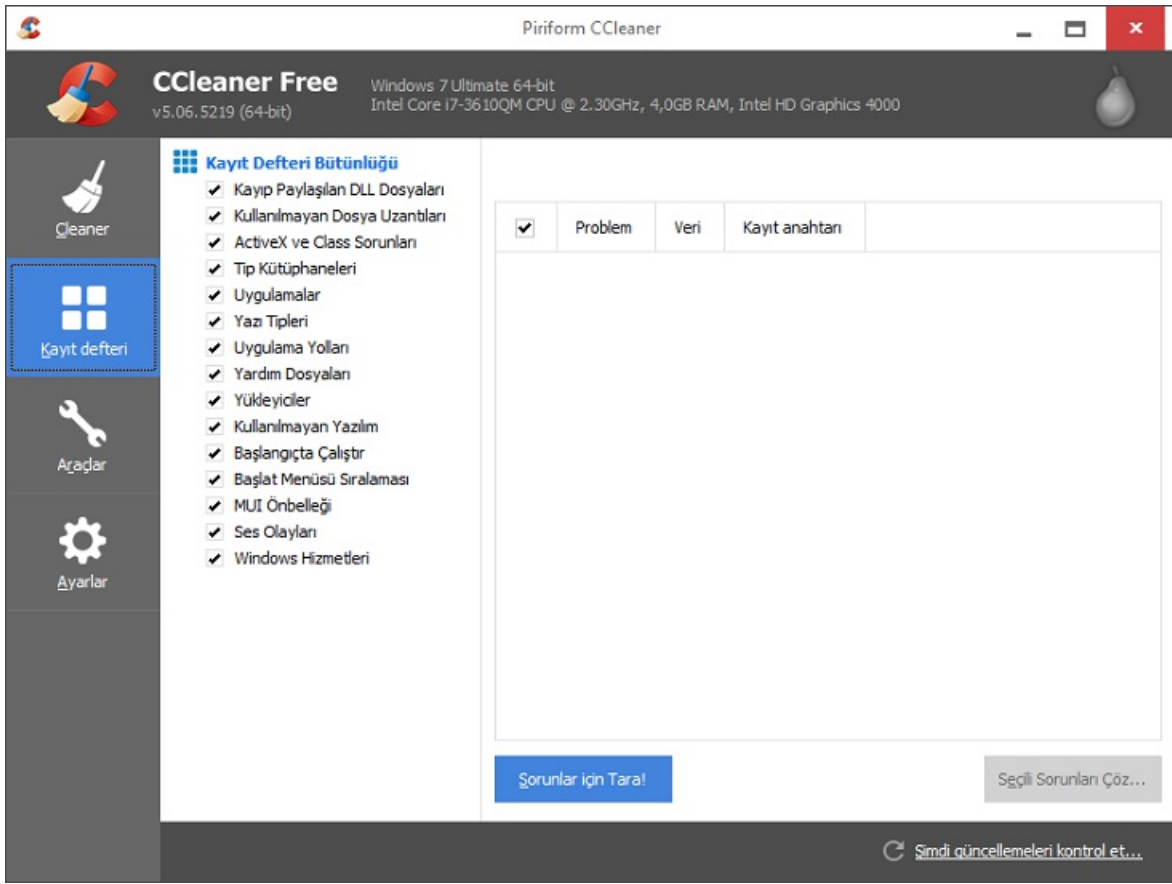
Zaman içinde, **Windows Kayıt Defteri** zamanı geçmiş yapılandırma bilgi ve ayarlarını, kullanılmayan programların izlerini biriktirir. **CCleaner Kayıt Defteri** seçeneği bu tip bilgileri gözden geçirmenize ve silmenize olanak verir. Böylece, sisteminizin genel işlevini ve hızını geliştirmiş ve dijital gizliliğinizi ve güvenliğinizi korumuş olursunuz.

**İpucu:** **Windows Kayıt Defteri** taraması haftada bir ya da ayda bir yapılmalıdır.

### 4.1 Windows Kayıt Defteri CCleaner Kullanarak Nasıl Temizlenir



**1. Adım.** Aşağıdaki ekranı etkinleştirmek için **Kayıt defteri** butonuna tıklayın:



\*Şekil 1: Kayıt Defteri modunda CCleaner kullanıcı arayüzü \*

**CCleaner Kayıt Defteri** penceresi, *Kayıt Defteri Bütünlüğü* listesi ve tespit edilen problemler ile ilgili bilgileri gösteren bir sekmeye ayrılmıştır.

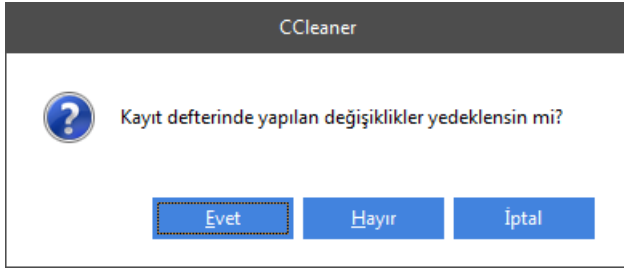
**2. Adım.** *Kayıt Defteri Bütünlüğü* listesindeki maddeleri **işaretleyin** (Şekil 1'de görüldüğü gibi) ve **ıkılayın**. Bu şekilde, kayıt ile ilgili problemler çözülmek üzere taranacaktır. Bir süre sonra sonuçlar şu şekilde görünür:

| 100%                                |                          |          |                                                                           |
|-------------------------------------|--------------------------|----------|---------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | Problem                  | Veri     | Kayıt anahtarı                                                            |
| <input checked="" type="checkbox"/> | Kullanılmayan Dosya...   | .eml     | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\eml      |
| <input checked="" type="checkbox"/> | Kullanılmayan Dosya...   | .lng     | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\lng      |
| <input checked="" type="checkbox"/> | Kullanılmayan Dosya...   | .wdseml  | HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\wdseml   |
| <input checked="" type="checkbox"/> | Geçersiz Varsayılan ...  | C:\W...  | HKCR\WLANImportFile\DefaultIcon                                           |
| <input checked="" type="checkbox"/> | Birlikte Aç sorunu       | D:\Pr... | HKCR\WLANImportFile\shell\Open                                            |
| <input checked="" type="checkbox"/> | ActiveX ve Class Sor...  | Local... | HKCR\CLSID\{29F458BE-8866-11D5-A3DD-00B0D0F3BAA7}                         |
| <input checked="" type="checkbox"/> | ActiveX ve Class Sor...  | InPro... | HKCR\CLSID\{5E688170-BDC7-48AA-A339-5F74CFDBDC9C}                         |
| <input checked="" type="checkbox"/> | ActiveX ve Class Sor...  | InPro... | HKCR\CLSID\{6EDCD38E-8861-11D5-A3DD-00B0D0F3BAA7}                         |
| <input checked="" type="checkbox"/> | ActiveX ve Class Sor...  | InPro... | HKCR\CLSID\{CE8A3669-40C7-4F4E-9B9B-AA3DD10DAC10}                         |
| <input checked="" type="checkbox"/> | ActiveX ve Class Sor...  | InPro... | HKCR\CLSID\{5E688170-BDC7-48AA-A339-5F74CFDBDC9C}                         |
| <input checked="" type="checkbox"/> | Kullanılmayan kayıt ...  | migwi... | HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\migwiz.exe       |
| <input checked="" type="checkbox"/> | Uygulama Yolu Sorunu     | D:\Js... | HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\C...     |
| <input checked="" type="checkbox"/> | Uygulama Yolu Sorunu     | D:\Js... | HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\C...     |
| <input checked="" type="checkbox"/> | Uygulama Yolu Sorunu     | D:\Js... | HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\C...     |
| <input checked="" type="checkbox"/> | Uygulama Yolu Sorunu     | D:\Js... | HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\C...     |
| <input checked="" type="checkbox"/> | Uygulama Yolu Sorunu     | D:\Js... | HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\C...     |
| <input checked="" type="checkbox"/> | Kullanılmayan yazılım... | Piriform | HKLM\Software\Piriform                                                    |
| <input checked="" type="checkbox"/> | Geçersiz güvenlik-du...  | {034...  | HKLM\SYSTEM\ControlSet002\services\SharedAccess\Parameters\FirewallP...   |
| <input checked="" type="checkbox"/> | Kayıp MUI Kaynağı        | D:\Pr... | HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\... |

Şekil 2: Çözülecek problemler listesini gösteren sonuç sekmesi

**Windows Kayıt Defterini** temizlemeye başlamadan önce almanız gereken bir önlem, kayıt defterinizi yedeklemektir. **Windows Kayıt Defteri** temizlendikten sonra bir problem olursa, yedekleme dosyalarınızı kullanarak **Windows Kayıt Defterinizi** eski haline getirebilirsiniz.

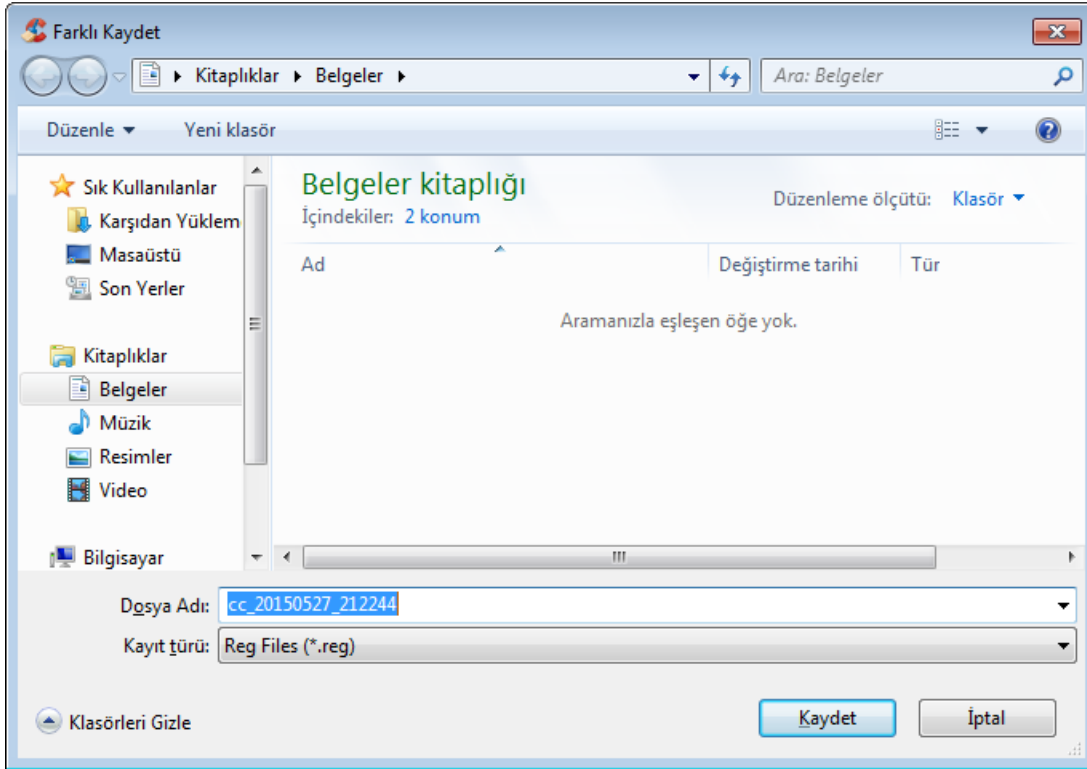
3. Adım. Aşağıda görünen iletişim kutusunu etkinleştirmek için [Seçili Sorunları Çöz...](#) ü tıklayın:



Şekil 3: Onay iletişim kutusu

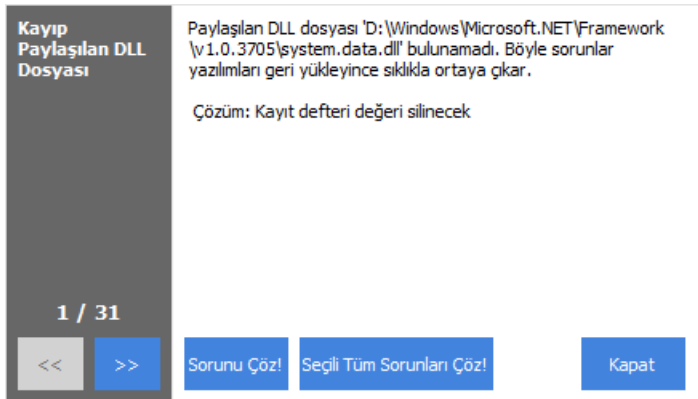
**İpucu:** Yedek kayıt defterini nereye sakladığınızı unutursanız, .reg dosya uzantısını aratabilirsiniz.

4. Adım. Kayıt defterinizi yedeklemek için [Evet](#) i tıklayın ve aşağıdaki ekranı etkinleştirin:



Şekil 4: Farklı Kaydet yer belirleme tarayıcısı

5. Adım. Dosyanızı yedeklemek için bir yer belirledikten sonra [Kaydet](#) i tıklayın ve aşağıdaki iletişim kutusunu etkinleştirin:



Şekil 5: Sorunu çöz/Seçili Tüm Sorunları çöz iletişim kutusu

**Not:** Gelişmiş veya uzman kullanıcılar, ihtiyaçlarına göre, bazı problemleri çözerken bazılarını yok saymak isteyebilirler. Ortalama düzeydeki yeni kullanıcıların tüm seçili problemleri çözmesini tavsiye ederiz.

**6. Adım.** Sorunları teker teker görüntülemek için << veya >> figürlerini **tıklayın** ve daha sonra çözmek istediğiniz sorunları seçerek **Sorunu Çöz**ü tıklayın.

**7. Adım.** Seçilen tüm problemleri çözmek için **Seçili Tüm Sorunları Çöz**ü **tıklayın** ve temizleme işlemini tamamlamak için **Kapat**ı **tıklayın**.

**İpucu:** Çözülecek problem kalmayana kadar **2. Adım** ile **7. Adım** arasındaki adımları tekrar edin.

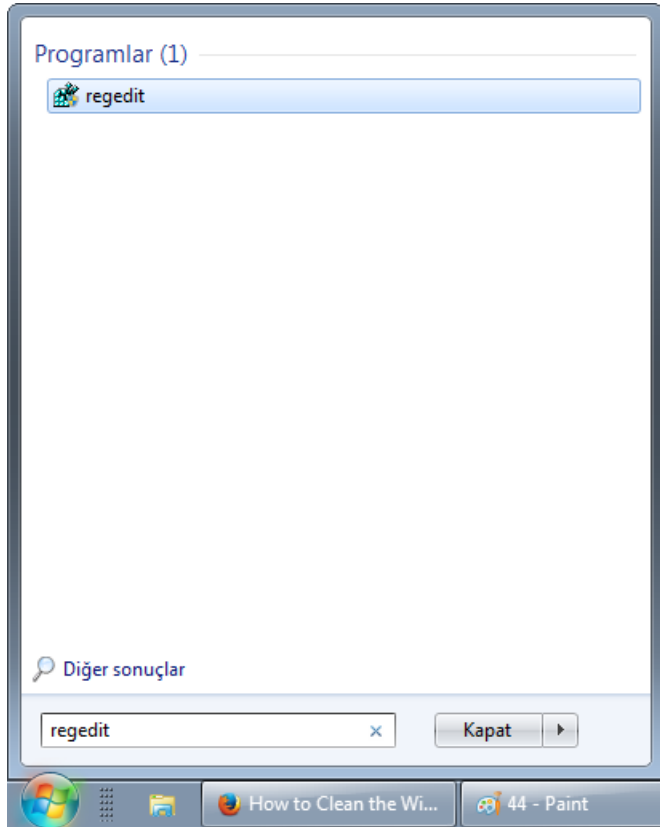
Böylelikle, Windows Kayıt Defteri başarılı bir şekilde temizlenmiştir.

## 4.2 Kayıt Defterinin Yedekleme Dosyası Nasıl Geri Kazanılır?

**Windows Kayıt Defteri'ni** temizlemenin sisteminizin işleyişinde bir soruna yol açtığını düşünüyorsanız, **4.1** bölümünün **üçüncü ile beşinci adım** arasında yarattığınız kayıt defteri yedekleme dosyasını kullanarak orijinal kayıt defterinizi geri getirebilir ve sisteminizin sorunlarını giderebilirsiniz.

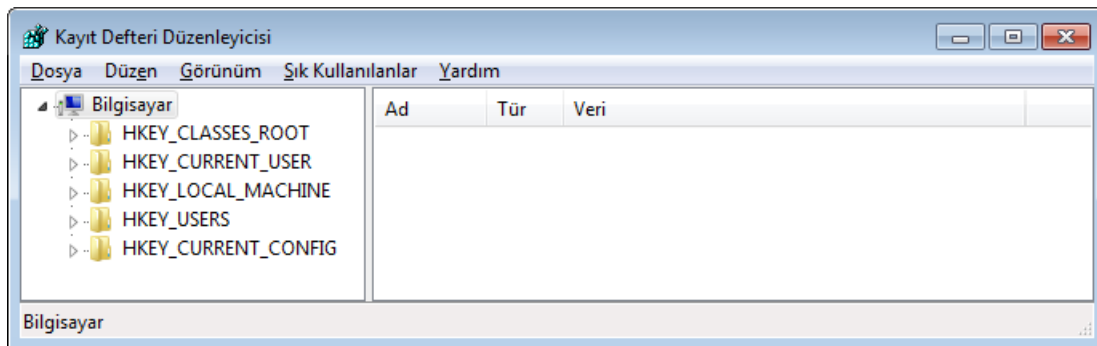
Orijinal kayıt defterini geri getirmek için aşağıdaki adımları takip ediniz:

**1. Adım.** *Çalıştır* penceresini etkinleştirmek için **Başlat > Çalıştır**'ı seçin ve aşağıda görüldüğü gibi *regedit* yazın:



Şekil 6: Çalıştır penceresi

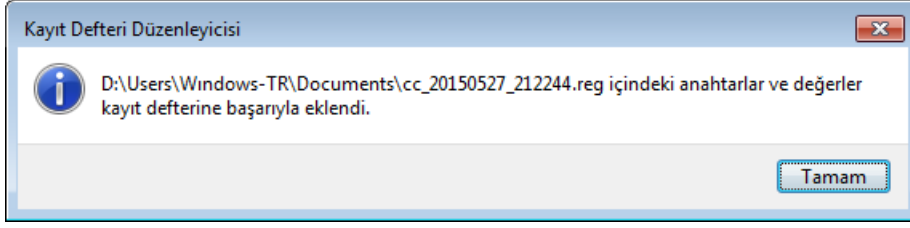
**2. Adım.** Aşağıdaki ekranı etkinleştirmek için **Tamam**ı **tıklayın**:



Şekil 7: Kayıt Defteri Düzenleyicisi

**3. Adım.** *Kayıt Defteri Dosya Aktar* ekranını etkinleştirmek için \*Kayıt Defteri Düzenleyicisi menüsünden **Dosya > İçer Aktar**'ı seçin ve daha sonra  cc\_20150527\_212244 'ü seçin.

**4. Adım.** Aşağıdaki iletişim kutusunu etkinleştirmek için  'ı tıklayın:



Şekil 8: Kayıt Defteri yedeklemenin gerçekleştiğini onaylayan Kayıt Defteri Editörü iletişim kutusu

**5. Adım.** Kayıt Defteri yedekleme dosyasını geri getirme işlemini tamamlamak için  'ı tıklayın.

## Taşınabilir CCleaner

### Short Description:



**CCleaner**, dijital gizlilik ve güvenliğinizi korumak için hayati öneme sahip, kullanımı kolay ve etkin bir programdır. **CCleaner**, tarayıcı geçmişinizi, çerezlerinizi ve çalışma oturumunuz esnasında oluşturulmuş diğer geçici dosyaları ve diskinizdeki boş alanları kalıcı olarak silerek veya temizleyerek, sisteminizi kötü etkileyen ve çalışma alışkanlıklarınızı ve tercihlerinizi kontrol eden partileri sınırlar.

### 5.1 Taşınabilir CCleaner'ın Kurulu ve Taşınabilir Versiyonları Arasındaki Farklar

Taşınabilir araçların lokal bilgisayarlara kurulu *olmadığı* için, varlıkları ve kullanımları kolayca tespit edilemez. Fakat, aklınızda tutun ki, taşınabilir USB aracınızı ve diğer taşınabilir aletleriniz ancak kullandığınız bilgisayar kadar güvenlidir ve reklam destekli bilgisayar yazılımlarına, kötü amaçlı yazılımlara, casus yazılım ve virüslere açıktır.

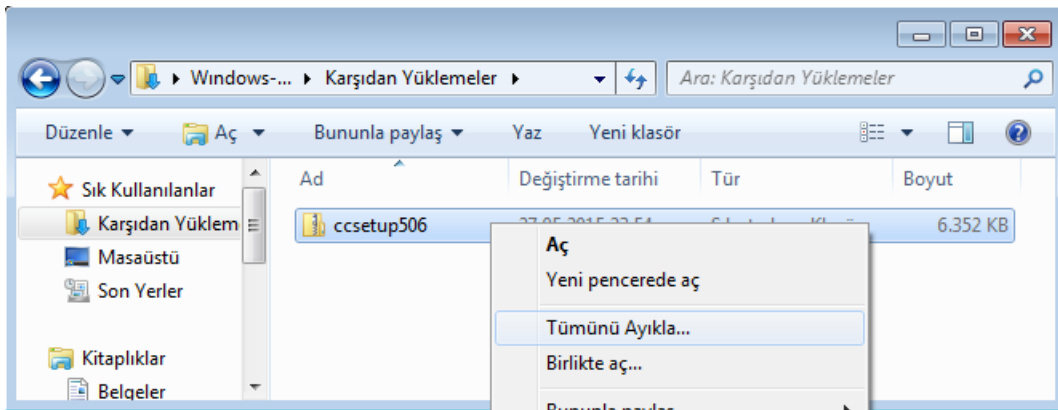
Bunların dışında **Taşınabilir CCleaner**'ın bir farkı yoktur ve lokal bir bilgisayara da kurulabilir.

### 5.2 Taşınabilir CCleaner Nasıl İndirilir ve Paketinden Çıkarılır?

Taşınabilir CCleaner'ı indirmek ve paketinden çıkarmak için aşağıdaki adımları takip edin:

**1. Adım.** <http://www.piriform.com/ccleaner/download/portable> <sup>[64]</sup> bağlantısına **tıklayın** ve ilgili **Taşınabilir CCleaner** indirme sitesine gidin. Bu sayede **Taşınabilir CCleaner**'i otomatik olarak indirmeye başlayabilirsiniz.

**2. Adım.** İndirdiğiniz klasöre gidin ve  ccsetup506 'nın üzerine **çift tıklayın**. Açılan Windows açılır menüsünden, aşağıdaki *Şekil 1*'de görüldüğü gibi **Tümünü Ayıkla**'yı seçin.



Şekil 1: *Tümünü Ayıkla...* maddesi seçili Windows menüsü

**Not: 2. Adım** Sıkıştırılmış Klasörleri Ayıkla penceresini etkinleştirecektir:

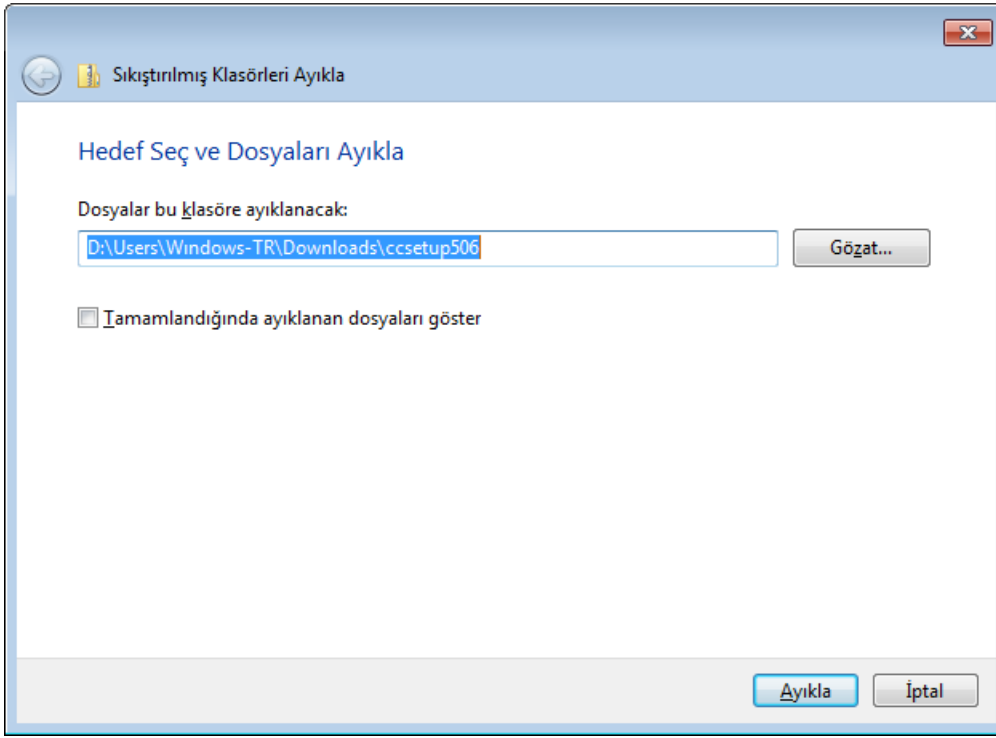
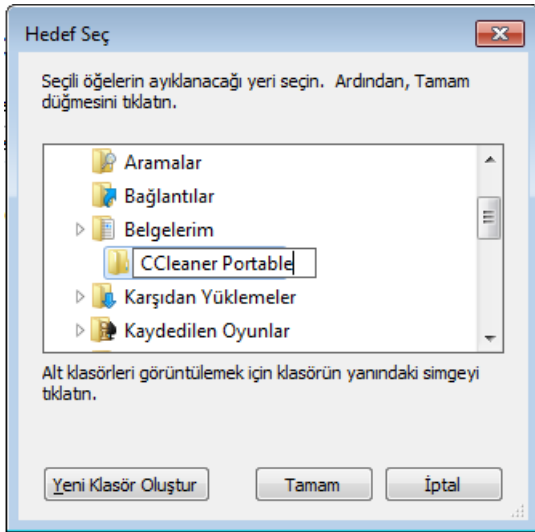


Figure 2: Hedef Seç ve Dosyaları Ayıkla Penceresi

**3. Adım.** Hedef Seç penceresini etkinleştirmek için **Gözet...**’ı **tıklayın** ve taşınabilir aracınıza veya USB hafıza çubuğunuza **gidin**. Kurulum dosyasını çıkarmak için yeni **Taşınabilir CCleaner** dosyası yaratmalısınız. Bunun için **Yeni Klasör Oluştur**’u **tıklayın**.

**4. Adım.** Aşağıdaki **Şekil 3**’te görüldüğü gibi, yeni dosyanıza dosya ağacında bir isim **girin**.

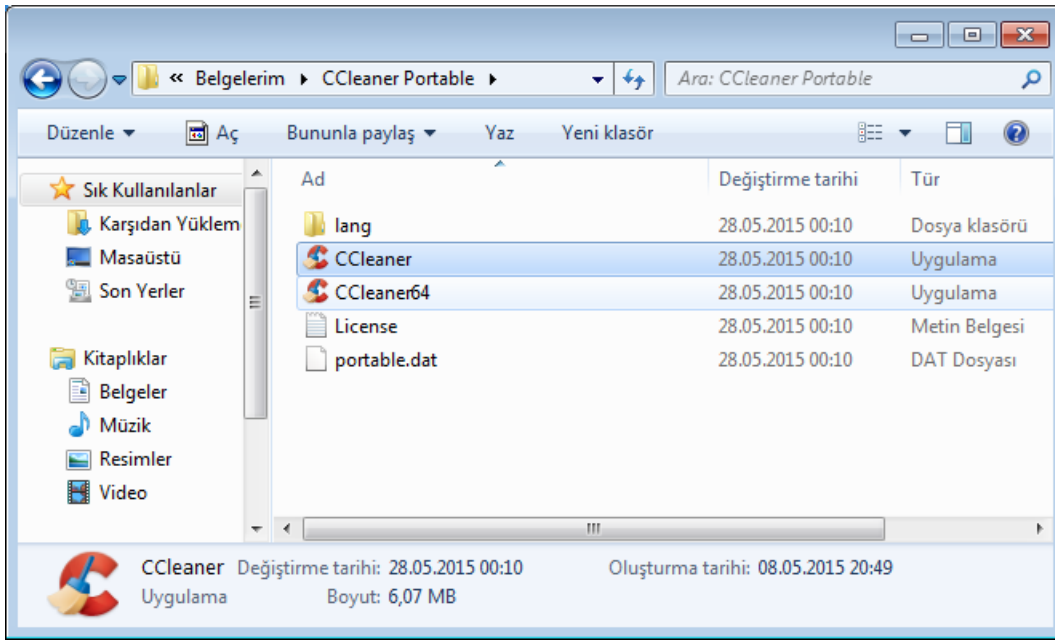


Şekil 3: Hedef Seç penceresi

**Not:** Taşınabilir CCleaner dosyası için farklı bir isim seçerseniz onu kullandığınız daha az belli olacaktır.

**5. Adım.** Hedef Seç penceresini kapatmak için **Tamam**’ı **tıklayın** ve **Hedef Seç ve Dosyaları Ayıkla** penceresine dönün. Sıkıştırılmış dosyanın içeriğini yeni yarattığınız dosyaya çıkartmak için **Ayıkla**’yı **tıklayın**.

**6. Adım.** **Taşınabilir CCleaner**’ın başarılı bir şekilde belirlenen dosyaya çıkarıldığında **Şekil 4**’te görünen ekran otomatik olarak etkinleşir:



Şekil 4: Taşınabilir diskte hedeflenen dosyaya çıkarılmış CCleaner programı

7. Adım. Taşınabilir CCleaner'ı başlatmak için  'a çift tıklayın..

Programı yapılandırmak ve kullanmak için lütfen **CCleaner** [65] bölümüne bakın.

#### Offline Installation Instructions :

#### CCleaner Kurma

- Kısa **Uygulamalı Rehberler'in** [1] Giriş bölümünü okuyun
- Aşağıdaki **CCleaner** ikonunu **tıklayın** ve yükleyiciyi 'Aç'ın veya 'Çalıştır'ın. Gerekirse yükleyiciyi önce kaydedin, daha sonra üzerine çift tıklayın
- Devam etmeden önce bir sonraki bölümdeki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulum gerçekleştikten sonra silebilirsiniz

CCleaner:



[66]

## Gelişmiş Seçenekler, Sıkça Sorulan Sorular ve Gözden Geçirme

Bu sayfadaki kısımların listesi:

- **6.0 Gelişmiş Seçenekler**
- **6.1 CCleaner Kullanarak Nasıl Program Kaldırılır?**
- **6.2 CCleaner'la Başlangıç Programları Nasıl Devre dışı Bırakılır?**
- **6.3 CCleaner Kullanarak Boş Disk Alanı Nasıl Temizlenir?**
- **6.4 Sık Sorulan Sorular ve Özet**
- **6.5 Özet Soruları**

## Gelişmiş Seçenekler

Bilgisayar sisteminizin etkin çalışmasını sağlayan iki **CCleaner** özelliği vardır. Bunlar aşağıda açıklandıkları gibi Geri Yükle (Kaldır) ve Başlangıçta özellikleridir . Bu bölümde ayrıca belirlenen bir diskteki boş alanları nasıl yok edeceğinizi veya öğrenebilirsiniz.

### 6.1 CCleaner Kullanarak Nasıl Program Kaldırılır

**Önemli:** Sileceğiniz veya kaldıracağınız programın bilgisayarınızın genel işleyişi için önemli olmadığından emin olun.

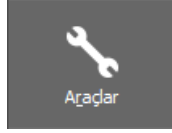
**CCleaner'**ı başlatmadan önce, daha önce kurduğunuz fakat kullanmadığınız veya istemediğiniz yazılımları silerek, onların

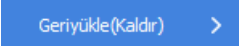
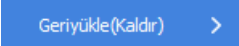
geçici dosyalarını ve klasörlerini de silmiş olursunuz. Bu sayede, silinecek olan geçici dosya ve klasör sayısını ve temizleme işleminin süresini azaltmış olursunuz.

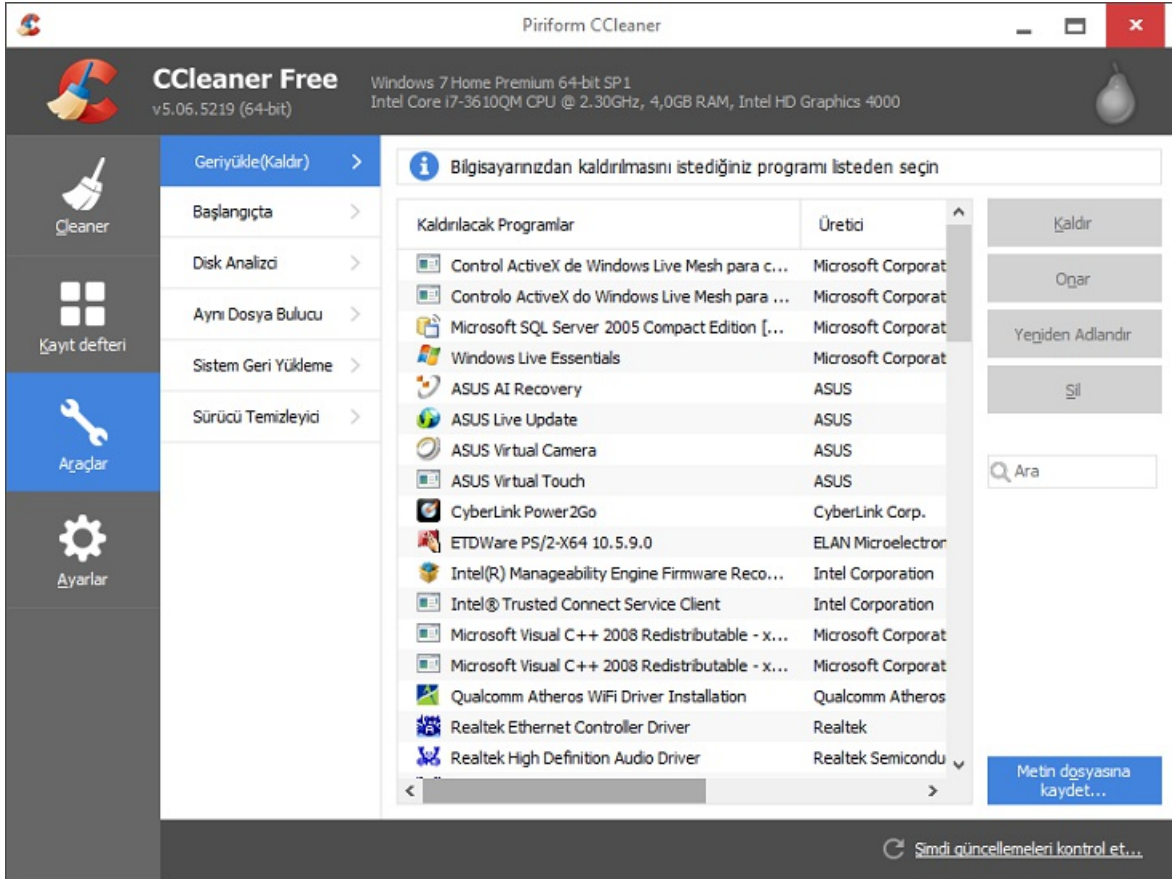
**CCleaner Program Kaldırma** özelliği, **Kontrol Panelinde** bulunan **Program Kaldırma** özelliği ile aynı işlevi görür. **CCleaner Program Kaldırma** özelliği programları daha etkin ve çabuk bir biçimde listeler.

Kullanılmayan programları kaldırmak için aşağıdaki adımları takip edin:

**1. Adım.** Piriform CCleaner konsolunu etkinleştirmek için 'a tıklayın ya da **Başlat > Programlar > CCleaner**'i seçin.

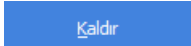


**2. Adım.** Aşağıdaki ekranı etkinleştirmek için 'a ve daha sonra 'a tıklayın.

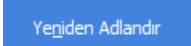
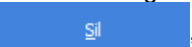


Şekil 1: Geri Yükle (Kaldır) sekmesini gösteren Araçlar opsiyonu

**\*\*Not:** Kaldırılacak Programlar listesinin sağında yer alan düğmeler, ancak kaldırılacak program seçildikten sonra etkin hale gelir.

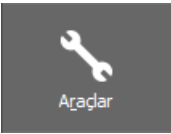
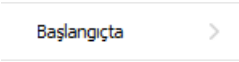
**3. Adım.** Kaldırılacak Programlar listesinden bir program **seçin** ve seçtiğiniz programı kaldırmak için 'a tıklayın.

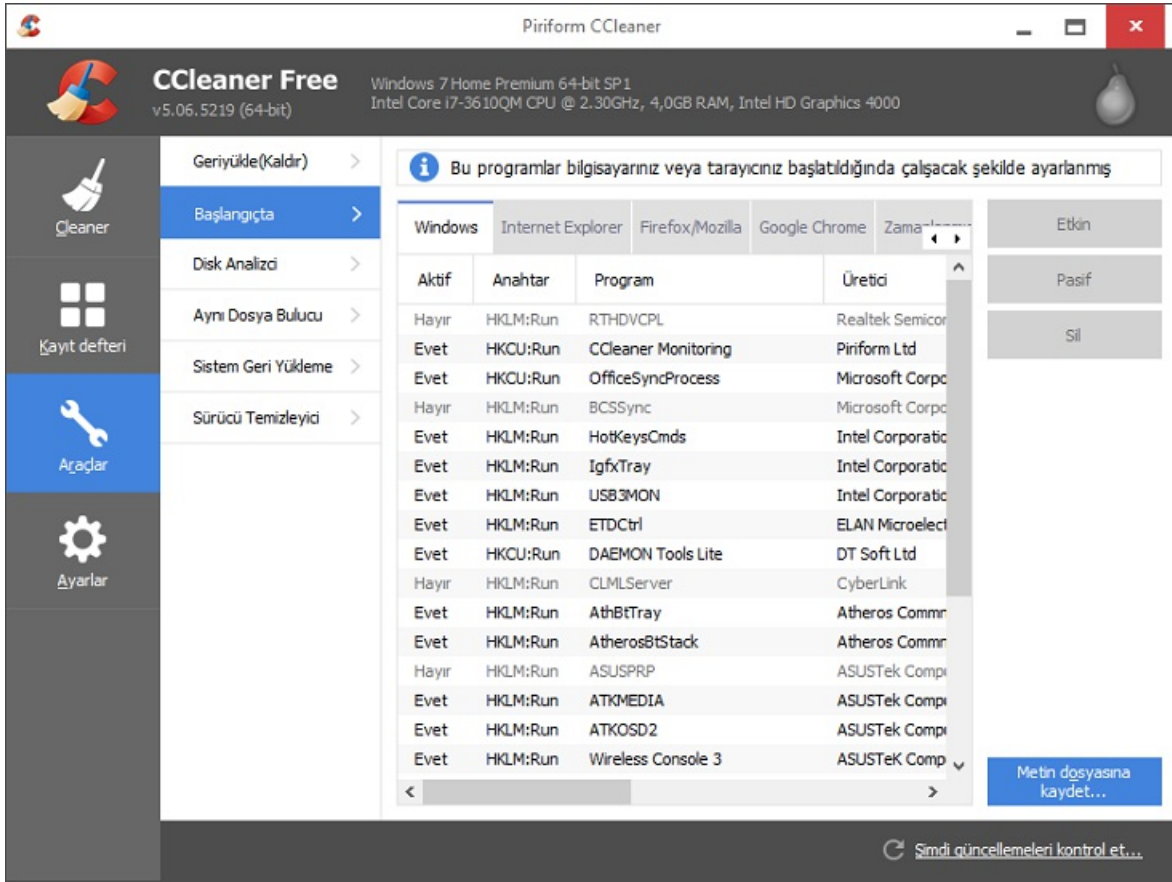
**İpucu:** Gelişmiş ve deneyimli kullanıcılar, belli bir yazılım korsanını saklayabilmek için **Yeniden Adlandır** ve **Sil** özelliklerini faydalı bulabilirler. Bu programlardan her biri bu programın varlığından bir tek sizin haberdar olmanızı sağlar ve sizi kurulmuş programları listeleyebilecek zararlı taraflardan korur.

**4. Adım.** Programa yeni bir isim vermek için 'a tıklayın ya da programı kaldırmadan listeden silmek için 'i tıklayın.

## 6.2 CCleaner'la Başlangıç Programları Nasıl Devre dışı Bırakılır

Başlangıç programları bilgisayarınızı başlattığınız zaman otomatik olarak başlar. Başlangıç, sınırlı sistem kaynaklarını kullanarak ve bilgisayarınızın başlama süresini uzatabilir.

1. Adım. Aşağıdaki ekranı etkinleştirmek için 'a ve daha sonra 'ya tıklayın.



Şekil 1: Başlangıçta bölümünü gösteren Araçlar seçeneği

2. Adım. Başlangıçta bölümünde listelenen programlardan birini **seçin** ve programı devre dışı bırakmak için 'i tıklayın. Böylelikle, bilgisayarınızı başlattığınız zaman bu program otomatik olarak başlamayacaktır.

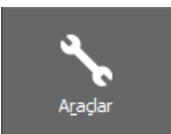
## 6.3 CCleaner Kullanarak Boş Disk Alanı Nasıl Temizlenir

**Windows** işletim sisteminde, bir dosyayı silmek sadece o dosyaya verilen referansı silmek anlamına gelir ve programın gerçek verilerini devre dışı bırakmaz. Zaman geçtikçe sürücünüzün bu kısmına yeni veriler yazılacaktır ama bilgili bir kullanıcı bu dosyanın bir kısmını veya tümünü yeniden oluşturabilir. Bunun olmasını engellemek için sabit diskinizdeki bu alanı temizlemeniz gerekir. **CCleaner** aynı zamanda **\*\*Ana Dosya Cetvelini (Master File Table, MFT) \*\*** temizlemenize olanak sağlar.

**Ana Dosya Cetvelini (Master File Table, MFT)**, tüm dosyaların isim, yer ve diğer bilgilerini içeren bir dizindir. **Microsoft Windows** bir dosya sildiği zaman, verimlilik açısından, sadece bu dosyanın dizin girişini silinmiş gibi gösterir. Fakat dosyanın **MFT** girişi ve içeriği sabit diskinizde yer tutmaya devam eder.

**Not:** Disk ve **MFT** temizliği oldukça uzun sürer ve bu süre bu işlemde kaç geçiş (passes) yapıldığına göre değişir.

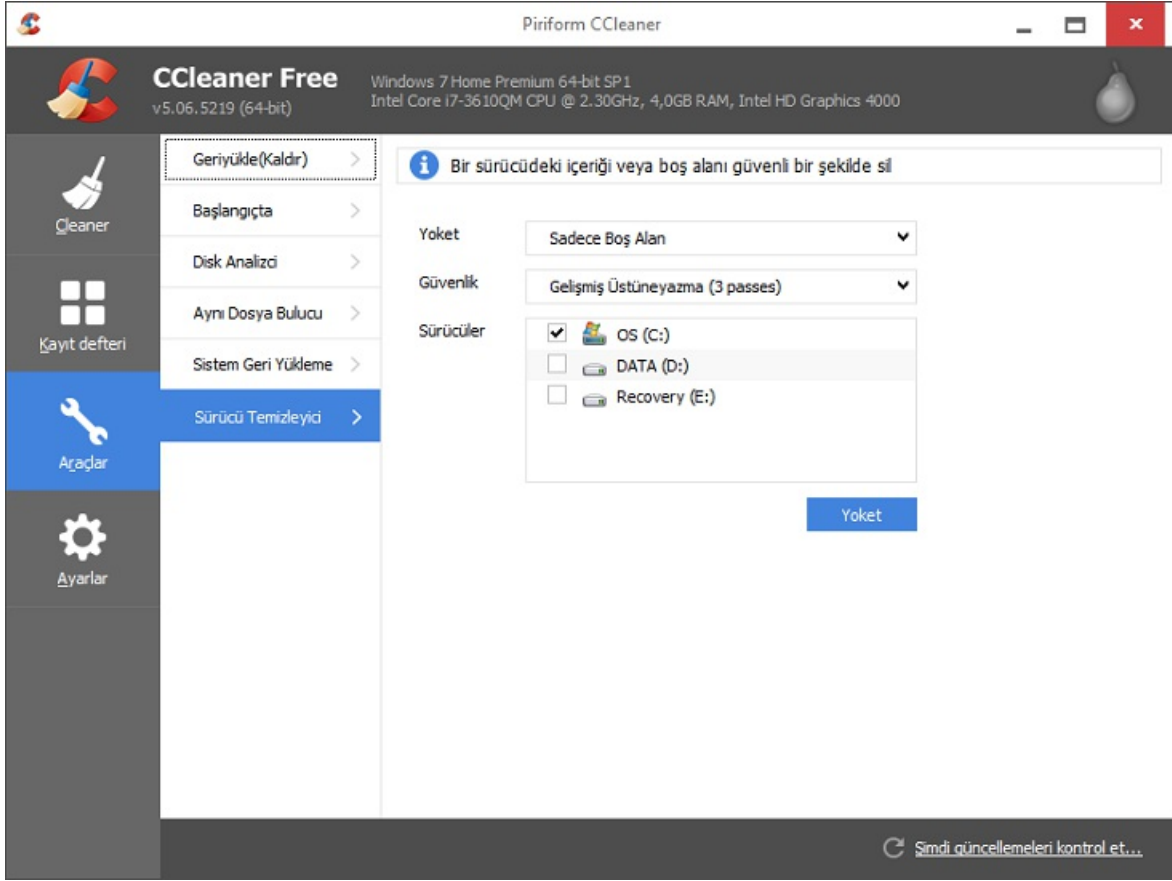
Bir sürücüyü temizlemek için aşağıdaki adımları takip ediniz:

1. Adım. 'a, sonra da 'ye tıklayın.

2. Adım. 'a **tıklayarak** aşağı açılır listeyi etkinleştirin ve **Sadece Boş Alan** veya **Tüm Sürü (Bütün bilgiler silinecek)** seçeneklerinden birini **seçin** ve Güvenlik aşağı açılır menüsünden 'yı **seçin**.

**Uyarı:** Tüm belge, dosya, klasör ve boş alanlarınızın silinmesini istediğinizden **tamamen** eminseniz **Tüm Sürü (Bütün bilgiler silinecek)** seçeneğini seçin.

**3. Adım.** Silinecek sürücü ile ilişkili işaret kutucuğunu **işaretleyin** ve **Yoket** i etkinleştirin. Aşağıdakine benzer bir pencere ile karşılaşacaksınız:



Şekil 3: İlgili seçenekleri etkinleştirmiş Sürücü Temizleyici bölümü

**4. Adım.** Seçtiğiniz disk(ler)in temizliğini başlatmak için **Yoket** i seçin.

## 6.4 Sık Sorulan Sorular ve Gözden Geçirme

**Soru:** CCleaner'ı devre dışı bırakırsam, daha önce silmiş olduğum materyal silinmiş olmaya devam eder mi?

**Cevap:** Evet, CCleaner'ı düzgün bir şekilde yapılandırdıysanız, sildiğiniz dosyalar kalıcı olarak silinir.

**Soru:** CCleaner'ı bir USB çubuğuna kopyalarsam, bir İnternet kafede yapmış olduğum işlemlerin izlerini o bilgisayarda silebilir miyim? Bu şekilde kullanmanın bir sakıncası var mı?

**Cevap:** Yok, hayır, bu şekilde kullanılabilir. **CCleaner'in taşınabilir bir versiyonu** <sup>[67]</sup> vardır. Çalıştığınız İnternet kafe, USB hafıza çubuğundan program kullanımına izin veriyorsa, orada yaptığınız işlemlerin izlerini silmek için **CCleaner** kullanabilirsiniz. Yine de İnternet kafede izlenebileceğinizi aklından çıkarmayın. Ayrıca, USB hafıza çubuğunu İnternet kafedeki bilgisayara bağlayarak virüslere açık hale getirmiş olduğunuzu unutmayın.

**Soru:** CCleaner ile temizlik yaparken sadece bir kere çalıştırırsam, verilerim başkaları tarafından yeniden oluşturulabilir mi? 7 geçişi (passes) kullanırsam nasıl bir değişiklik olur?

**Cevap:** TVerilerinizi temizlemek için ne kadar geçiş kullanırsanız, silmek istediğiniz verilerin tekrar bulunması o kadar zor hale gelir. Fakat, bu işlemi ne kadar çok kez tekrarlırsanız, silme işlemi de o kadar uzun sürer.

**Soru:** Windows Kayıt Defterini silmek, bilgisayarımda yakın zamanda kurduğum ve kullandığım programların izlerini silmek içi yeterli midir?

**Cevap:** İdeal olarak, programlara ait tüm dosyaları **CCleaner** kullanarak silmeniz gerekir. Bu sayede geçici dosyaları, **Kayıt Defterini** ve diskinizdeki boş alanları, kullandığınız yazılımların ve bunlarla yaptığınız işlemlerin izlerini de silebilirsiniz.

## 6.5 Gözden Geçirme Soruları

- CCleaner bilgisayarınızdan ne tür bilgileri siler?
- Bunu nasıl yapar?
- Verilerinizi güvenli bir şekilde gizlemek için bu işlemi kaç geçişle yapmalısınız?

- **Windows Kayıt Defteri** nedir ve neden temizlenmesi önerilir?
- **Windows Kayıt Defteri**'ni temizlemeden önce neler yapmalısınız?

# RiseUp - Güvenli E-posta Servisi

## Short Description:



RiseUp politik ve sosyal adalet için çalışan kişiler ve kurumlar için servisler sunan ve özel ve güvenli e-posta sağlayan kolektif bir organizasyondur.

## Ana Sayfa

<https://riseup.net/> <sup>[68]</sup>

## Bilgisayar Gereksinimleri

- İnternet bağlantısı
- **RiseUp** en uyumlu **Firefox** web tarayıcısı ile çalışır

## Bu bölümün son güncellenme tarihi

- Ağustos 2014

## Lisans

- Ücretsiz Servis

## Gerekli Okuma

- Nasıl Yapmalı Kitapçığının 7. Bölümü, İnternet İletişiminizin Gizliliği Nasıl Korunur <sup>[51]</sup>

## Buradan sağlayacağınız faydalar:

- Topluluk odaklı tasarlanmış ve reklamlardan bağımsız bir e-posta hesabı
- E-postanıza internet veya herhangi bir e-posta programı üzerinden ulaşma ve şifrelenmiş bir bağlantı üzerinden özel e-posta iletişiminizi sağlama olanağı
- E-posta adresinizi değiştirme, e-posta gelen kutunuzun kapasitesini ayarlama ve başkalarını **RiseUp** kullanmaya davet etme olanağı

## Alternatif E-posta Servisleri:

**RiseUp** İnternet gizliliği ve güvenliğini savunan güvenilir kişiler tarafından geliştirilmiş güvenli bir e-posta servisi olmasına rağmen, alışılmışın dışında bir e-posta servisi kullanmanız dikkatleri istenmeyen bir şekilde üzerinize çekebilir. Bazı durumlarda ülkenizdeki popüler bir e-posta servisini kullanarak bu durumu engellemeniz anlamlı olabilir. Amaç, bunu yaparken minimum güvenlik gereksinimlerinden hiçbir şekilde taviz vermemenizdir. Bir e-posta servisi seçerken aşağıda belirtilen noktaları göz önünde bulundurmanızı tavsiye ederiz:

1. Bilgileri (giriş bilgileriniz ve e-postalarınız dahil olmak üzere) aktarmak için **şifrelenmiş kanalları** (**https** ve IMAP, POP3 ve SMTP'ler gibi diğer SSL şifrelenmiş protokol tipleri gibi) kullanmaya izin veriyor mu ve şifreleme ile ilgili herhangi başka bir problem çıkartıyor mu (örneğin şifreleme sertifikaları ile ilgili problemler)?
2. **E-posta sunucuları güvenli bir şekilde yönetiliyor mu?** Bilgileriniz en güvenli şekilde saklamak için en iyi yöntemleri kullanan profesyoneller tarafından mı işletiliyor? Onların herhangi bir amaç uğruna (ticari, politik, dini vb.) bilgilerinizi üçüncü şahısların erişimine **açmayacağına** güveniyor musunuz?
3. Sunucuların coğrafi konumlarını, **hangi ülkenin yargı sistemi altında olduklarını** ve şirketlerin nereye bağlı olduğunu biliyor musunuz? Bu bilgilerin sizin e-posta aktiviteleriniz ve bilgilerinizin gizlilik ve güvenlik ayarları açısından ne anlama geldiğini biliyor musunuz?

Dünyanın belli yerlerinde **Google Mail**, daha iyi bir 'kamufle olma' olanağı sunarak, (ticari doğası gereği) güvenliğinizden fazla ödün vermenizi gerektirmeyerek **RiseUp'a** iyi bir alternatif sunabilir.

## 1.1 Başlamadan önce bu araç hakkında bilmeniz gerekenler

**RiseUp**, politik ve sosyal adalet için çalışan kişiler ve kurumlar için gizli ve güvenli bir barındırma, listeleme ve posta servisleri sağlamaya adanmış bir kolektiftir. Servisleri ücretsiz olduğu için ve RiseUp aktiviteleriniz takip etmediği için, e-posta hesabınız, reklam odaklı ve güvenli olmayan sağlayıcılara kıyasla çok daha küçüktür. Yeni bir hesap, ancak hali

hazırda kullanıcı olan iki kişi tarafından gönderilen davet kodu ile oluşturulabilir. [RiseUp hakkında daha fazla bilgi alabilmek için sitelerini ziyaret edebilirsiniz](#) [69].

**RiseUp** sadece, bilgisayarınız ve sunucunuz arasında güvenli bir iletişim kuran **Güvenli Soket Katmanı (Secure Sockets Layer, SSL)** üzerinden çalışır. Bu güvenlik, e-postanızı güvenli **POP**, **IMAP** ve **SMTP** bağlantıları (e-posta istemci programların e-postalarınızı indirmek ve göndermek için kullandığı protokoller) üzerinden bir istemci programda okuduğunuz zaman sağlanır. **RiseUp Mozilla Thunderbird** ile uyumlu bir şekilde çalışır. **RiseUp** e-posta hesabınıza ulaşmak için **Mozilla Thunderbird**'ü nasıl indireceğinizi öğrenmek için lütfen **Thunderbird** [70] ile ilgili bölüme bakınız.

**RiseUp** e-posta hesaplarına ek olarak aşağıdakileri de sağlar:

- E-posta grup iletişimleri için **E-posta Listesi** [71];
- **CrabGrass** [72] adlı, gruplar ve ağlar arasındaki organizasyonu sağlamak için ve küresel adalet hareketinin ihtiyaçlarına göre tasarlanmış, kendi ücretsiz ve açık kaynak sosyal ağ uygulaması;
- **EtherPad** [73] adlı, birden fazla kullanıcının aynı anda aynı belge üzerinde çalışmasını sağlayan ortaklaşa belge düzenleme platformu;
- **OpenVPN** [74] İnternet'i **RiseUp** sunucuları üzerinden taramaya izin veren şifrelenmiş vekil sunucu. Vekil sunucular üzerine daha fazla bilgi edinmek için [İnternette nasıl anonim kalınır ve İnternet sansürü nasıl aşılr](#) [75] adlı 8. Bölüm'e bakınız;
- **Jabber/XMPP** [76] adlı hızlı mesaj, metin, ses ve video konuşma sunucusu. Bu sunucuyu, diğer programların yanı sıra [Jitsi](#) [77], [Pidgin](#) [78], [Adium](#), and [ChatSecure](#) gibi programlar aracılığıyla kullanabilirsiniz. [Diğer İnternet iletişim araçlarını güvenli kılmak](#) [79] veya 7. Bölüm, [İnternet iletişiminizin gizliliği nasıl korunur](#) [51] bölümüne bakabilirsiniz. .

## RiseUp Hesabı Nasıl Oluşturulur

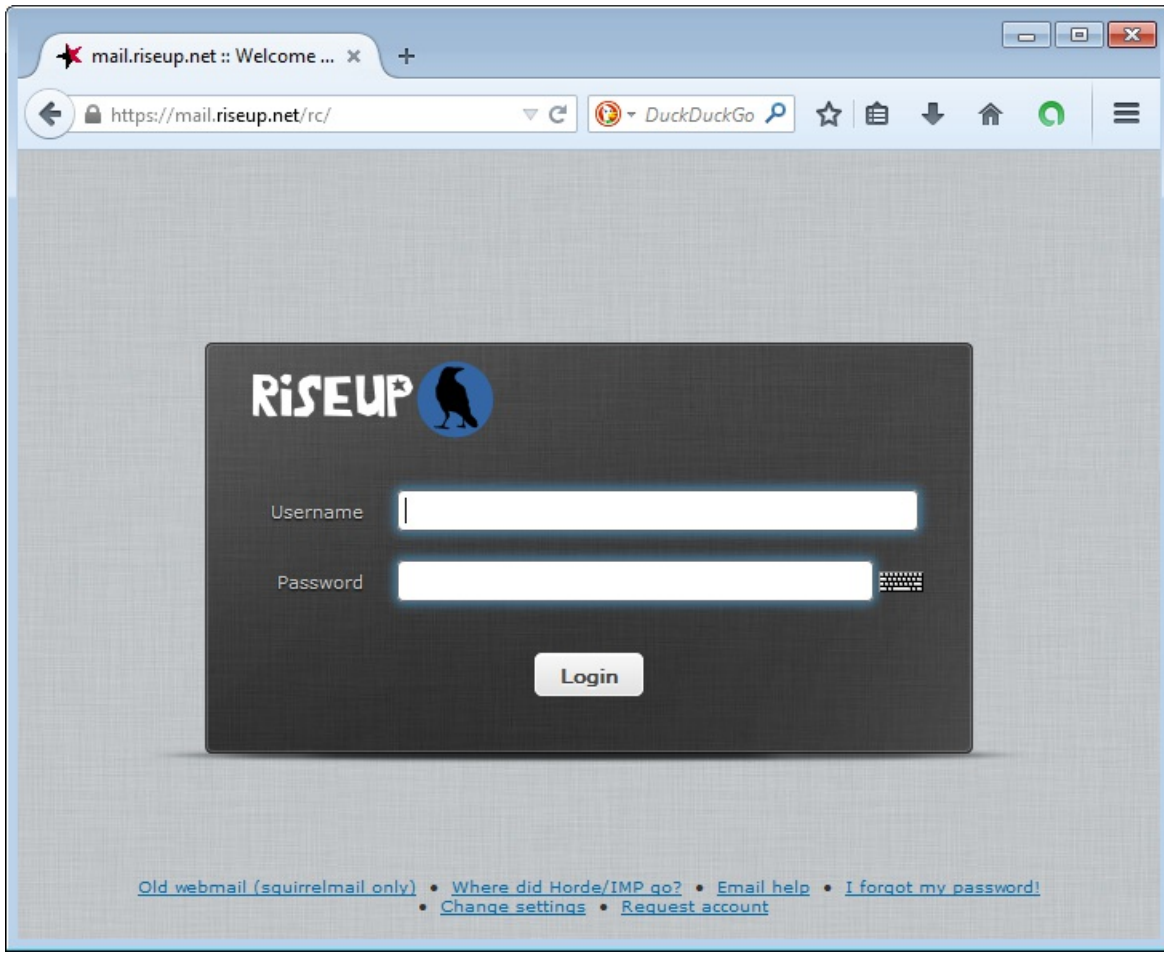
**RiseUp** bir e-posta hesabı oluşturmak için iki ayrı yöntem sunar. Her iki yöntem de kendine göre belli bir çaba ve zaman gerektirir.

1). **RiseUp** ekibinden direk olarak bir e-posta hesabı isteyebilirsiniz. Aklınızda tutun ki **RiseUp** büyük oranda bağışlar ve gönüllü çalışanların iyi niyet ve heyecanı ile ayakta durur – bu yüzden, bu yöntem herhangi bir hesabın normal onaylanma süresinden biraz daha uzun sürebilir.

2). Önerilen yöntem ise kişi ve/veya kurumların RiseUp hesabına sahip olan iki üye tarafından **RiseUp'a** katılmaya davet edilmesidir. Bu yöntemde her iki **RiseUp** üyesi size birer davetiye kodu gönderir. Bu kodların nasıl oluşturulduğunu görmek için lütfen [Kısım 4.3 Davetler Sayfası'na](#) [80] bakınız.

Davet kodlarınızı aldıktan sonra, ücretsiz **RiseUp** hesabınızı oluşturmak için aşağıdaki adımları takip ediniz:

**1. Adım. RiseUp** sitesini aşağıda görüldüğü gibi etkinleştirmek için web tarayıcınıza <https://mail.riseup.net> [81] yazın.



Şekil 1: <https://mail.riseup.net/page> sayfası

**Not:** <https://> adresindeki **s** artık **Güvenli Soket Katmanı (SSL)** üzerinden iletişim kurduğunuzu gösterir.

Bu konuda daha fazla bilgi edinmek için lütfen Kullanma Kılavuzu'ndaki **internet iletişiminizin gizliliği nasıl korunur** <sup>[51]</sup>, veya <https://help.riseup.net/security> <sup>[82]</sup> sayfasına bakınız.

**2. Adım.** [Request account](#) 'a **tıklayınız** ve *Hesap talep etme* sayfasını aşağıda görüldüğü şekilde etkinleştirin:



## Request an email account

This form will step you through the process of creating a riseup.net account. There are two ways to have your account approved: you can either get invite codes from existing users you know or wait for us to approve your request. It is sometimes difficult for us to keep up with the volume of requests, so it may take us up to a few weeks to get back to you. If you know two different riseup.net users, you can use the invite method, and your account will be created and be ready to use immediately. You should only request invites from people you know personally. Once you have completed this form, you cannot later go back and enter the invite codes. If you want to use the invite method, you need to get the codes before you fill out this form. To create codes, existing users can login to user.riseup.net and click 'Invites'.

<< Start Over

Next >>

Şekil 2: RiseUp e-posta hesabı talep etme sayfası

**3. Adım.** **RiseUp E-posta hesabı talep etme – E-posta servislerimiz hakkında** sayfasını görüntülemek için [Next >>](#) 'i tıklayın.

**Önemli:** Riseup hesap oluşturmada ilerleyebilmek için *E-posta servislerimiz hakkında* sayfasındaki tüm şart ve koşulları kabul etmelisiniz.

**4. Adım. RiseUp Sosyal Sözleşme, Gizlilik Politikası ve Hizmet Kullanım Şartları'nı** okuyunuz. Şart ve koşulları kabul ettiğinizi onaylamak için *Riseup.net*'i kabul ediyorum kutularını **işaretleyin**.

**5. Adım. Riseup** hesabınızı oluşturmaya başlamak için 'i **tıklayınız** ve şu çevrimiçi formları doldurunuz: *Hesap Bilgileri, Parola ve Etkinleştirme*.

**6. Adım.** Hesabınız için kullanmak istediğiniz kullanıcı adını **giriniz**. Bu ismi daha sonra girişte ve e-posta adresinizde kullanacaksınız. (Bu rehberdeki örnekte, **ssayyed@riseup.net** <sup>[83]</sup> e-posta hesabını oluşturmak için 'ssayyed' ismini kullandık).

**Önemli:** Kullanıcı adında virgöl, nokta veya boşluk kullanmayın.

The screenshot shows the 'Request an email account' form on the Riseup.net website. The form is titled 'Account information' and contains several sections:

- Username:** A text input field containing 'ssayyed'. To its right, a note states: 'Your username will determine your main email address. You can add other email aliases later.'
- Alternate email:** A large text input field. To its right, a note explains: 'If you forget your password, you will be able to have a new one mailed to one of these addresses. We can also use your alternate email addresses to contact you when you are unable to access your riseup.net account, and when your account request has been processed. If you do not fill out an alternate email, you will lose access to your account if you forget your password. You can specify more than one alternate email address---separate the addresses with a comma and a space.'
- Locale:** This section contains three sub-sections:
  - Language:** A dropdown menu showing 'english'. To its right, a note says: 'This setting determines your default language when using the user control panel.'
  - Country:** A dropdown menu. To its right, a note states: 'We use the country information to determine what languages we should support and where we should situate future servers. This information is entirely optional.'
  - Time Zone:** A dropdown menu. To its right, a note says: 'All times displayed in the user control panel will be shown for this time zone.'

At the bottom of the form, there are two buttons: '<< Prev' and 'Next >>'.

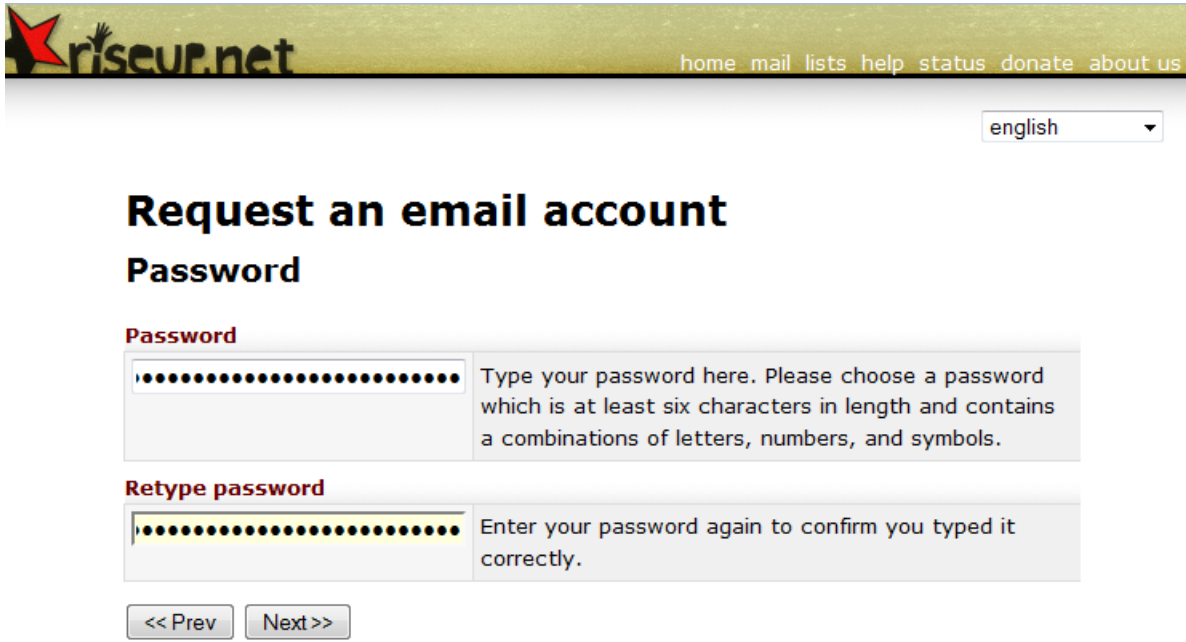
Şekil 3: Doldurulmuş bir Hesap Bilgileri Formu Örneği

**Dikkat ederseniz,** *Diğer e-posta, Dil, Ülke ve Zaman Dilimi* alanları değiştirilmemiş veya boş bırakılmıştır. Bunun sebebi sunucu üzerindeki kişisel bilgilerinizi mümkün mertebe azaltmaktır. *Diğer e-posta* alanını boş bırakmak gizliliği artırır, fakat bu hesabın parolasını unuttuğunuz takdirde sıfırlamanızı engeller.

**7. Adım.** Parola formuna gitmek için 'i tıklayınız.

**Not:** Seçtiğiniz kullanıcı adı daha önce alınmış ise başka bir kullanıcı adı seçmeniz istenecektir.

8. Adım. Parola ve Parolayı Yeniden Gir alanlarını **doldurunuz** ve **Next >>** 'i tıklayınız.



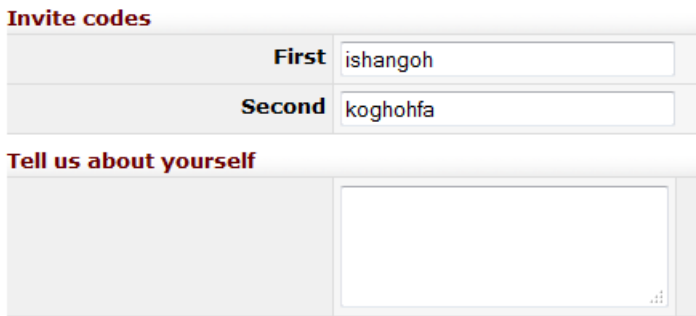
Şekil 4: Doldurulmuş Parola formu

**Önemli:** Riseup hesabınızın güvenliği açısından en önemli etken parolanızdır. Güçlü bir parolanın nasıl yaratılacağı konusunda Kullanma Kılavuzu'ndaki 3. Bölüm olan **Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** <sup>[4]</sup> ve **KeePass** <sup>[13]</sup> el kitabına bakabilirsiniz.

9. Adım. Etkinleştirme formunu doldurunuz.

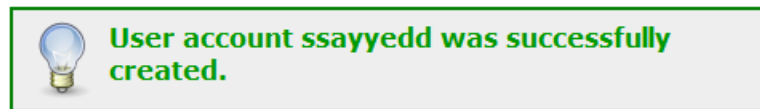
Davet kodlarını kişisel olarak tanıdığınız **RiseUp** hesap kullanıcılarından aldıysanız, girilmesi gereken alanlara davet kodlarını **girin**. Her Davet kodu farklı bir kullanıcıdan gelmelidir. Buna alternatif olarak, **RiseUp.net'ten**, *Bize kendinize dair birşeyler söyleyin* alanını doldurarak bir hesap isteyebilirsiniz. Davet kodlarınız varsa *Bize kendinize dair birşeyler söyleyin* alanını boş bırakın.

Davet kodlarını ilgili kutulara **girin**.



Şekil 5: Doldurulmuş bir Etkinleştirme formu örneği

10. Adım. **RiseUp** hesap isteme işlemini veya **RiseUp** hesap yaratma işlemini bitirmek için **Finish** 'i aşağıda görüldüğü gibi **tıklayın**:



Şekil 6: Hesabın başarı ile yaratıldığı onay örneği

11. Adım. **RiseUp** Hesap Ana Sayfa'sına dönmek için **Next >>** 'i tıklayın (Şekil 1'e bakınız).

Tebrikler! **RiseUp** e-posta hesabı isteğiniz veya yaratımınız başarı ile gerçekleşmiştir.

# RiseUp Hesabınıza Nasıl Giriş Yapılır?

Bu sayfadaki kısımların listesi::

- [3.0 RiseUp Hesabınıza Nasıl Giriş Yapılır?](#)
- [3.1 Sanal Klavye Nasıl Kullanılır?](#)

## 3.0 RiseUp Hesabınıza Nasıl Giriş Yapılır?

Hesabınıza girmek için aşağıdaki adımları takip ediniz:

**1. Adım.** RiseUp ana sayfasını aşağıda görüldüğü gibi SSL modunda açın: <https://mail.riseup.net/> <sup>[84]</sup>



Şekil 1: RiseUp posta giriş sayfası

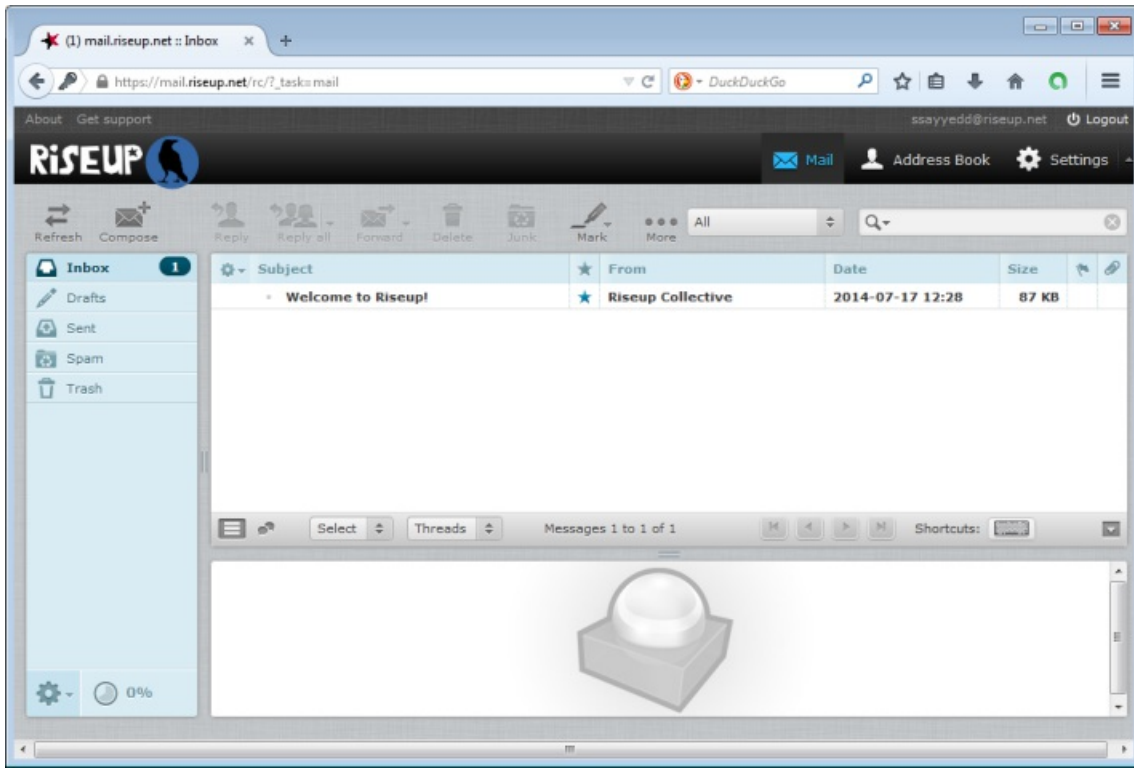
**Riseup** şu anda ücretsiz ve açık kaynak bir web posta arayüzü olan [Roundcube](#) <sup>[85]</sup> kullanmaktadır. Roundcube JavaScript gerektirir. Bunu kullanmak istemiyorsanız, **RiseUp** e-postalarınıza SquirrelMail üzerinden erişmenize de izin verir (aşağıya bakınız). RiseUp web posta tarayıcınızın çerezleri kabul etmesini ister (çerezler hakkında daha fazla bilgi edinmek için (see [Firefox bölümüne](#) <sup>[86]</sup> bakınız )

**RiseUp** web hesap giriş sayfasının ortasında giriş bölümü, alt kısımlarında ise bir dizi bağlantı vardır:

- [Eski web posta \(sadece squirrelmail ile\)](#) <sup>[87]</sup>: JavaScript gerektirmeyen, alternatif, basit ve hafif bir posta arayüzü;
- [Where did Horde/IMP go?](#) <sup>[88]</sup>: Önceden sunulan fakat artık kullanımda olmayan Horde/IMP web posta arayüzü;
- [E-posta yardım](#) <sup>[89]</sup>: Bir probleminiz olduğunda mutlaka okunması gereken bir bölüm;
- [Parolamı unuttum!](#) <sup>[90]</sup>: parolanızı tekrar kurmanızı sağlar;
- [Ayarları değiştir](#) <sup>[91]</sup>: [bir sonraki sayfaya bakın](#) <sup>[92]</sup>
- [Hesap talebi](#) <sup>[93]</sup>: [bir önceki sayfaya bakın](#) <sup>[94]</sup>

**2. Adım.** *Kullanıcı adı:* ve *Parola:* alanlarına bilgilerinizi **girin**. *Kullanıcı adı:* alanına **@riseup.net** kısmını **eklemeyiniz**.

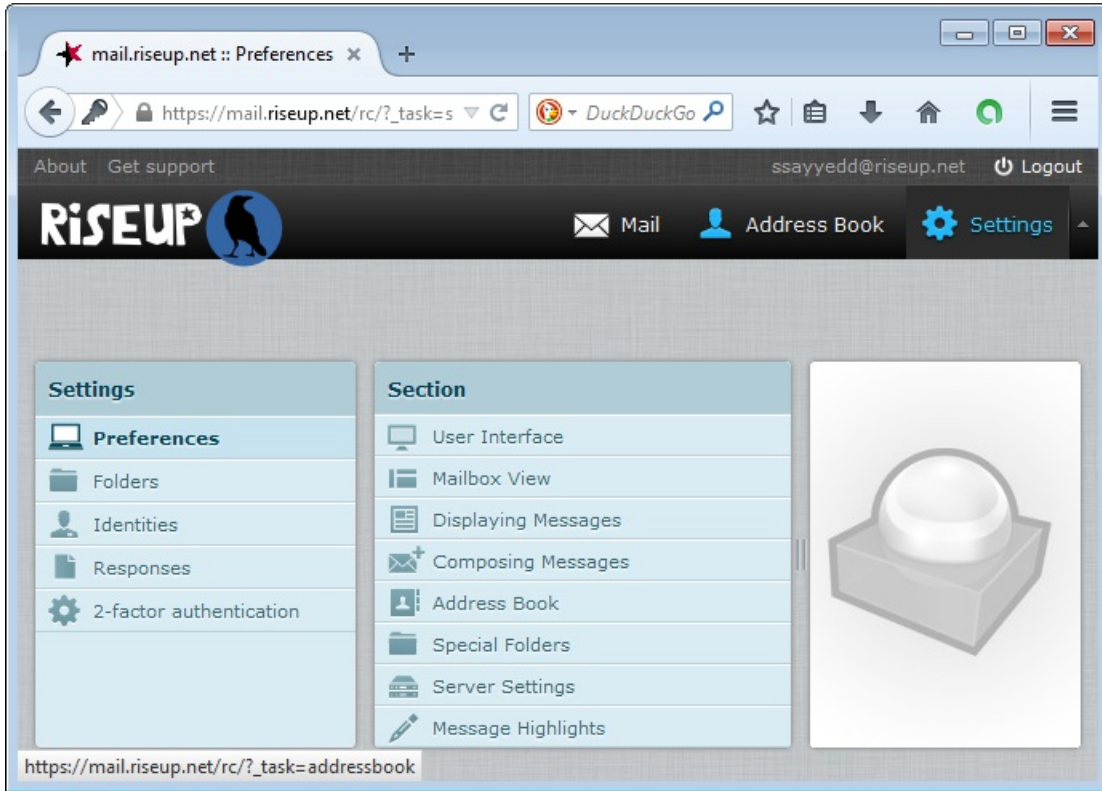
**3. Adım.** Hesabınızı aşağıda görüldüğü gibi açmak için sbos/screen/riseup-en-1/12.png'i **tıklayın**:



Şekil 2: RiseUp SquirrelMail Hesap örneği

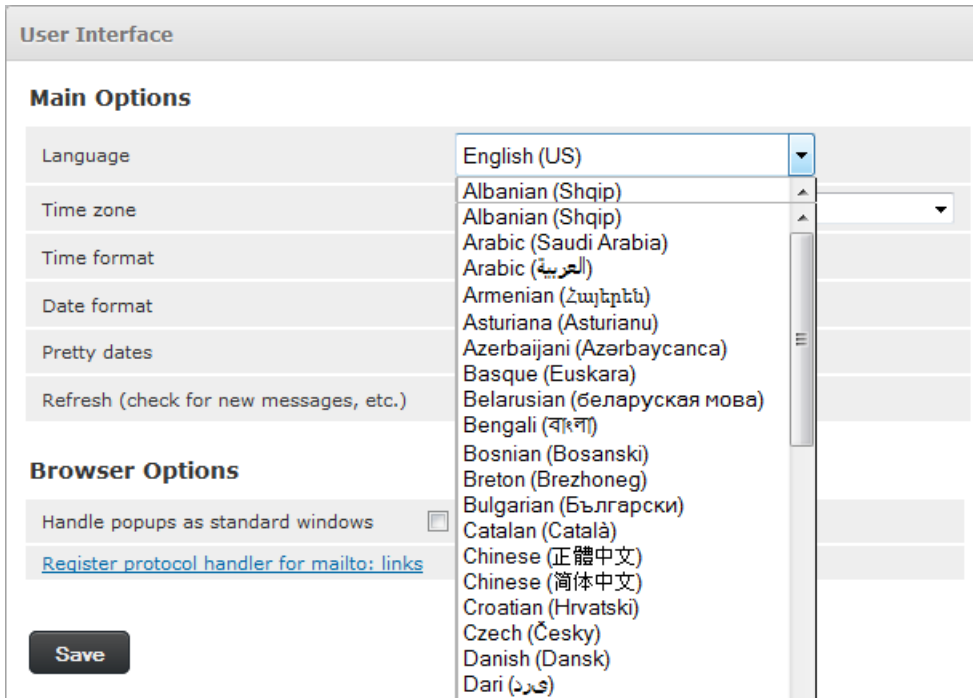
**Tercihe Bağlı Adımlar:** Web posta arayüzünüzü başka bir dile çevirmek istiyorsanız aşağıdaki tercihe bağlı adımları takip edebilirsiniz:

**3. Adım.** Üst menüden  **Settings**’i seçin. Ayarlar penceresi aşağıda görüldüğü gibi açılacaktır:



Şekil 3: Ayarlar bölümü

**4. Adım.**  **User Interface**’i seçerek **Kullanıcı Arayüzü** ayarları bölümünü aşağıdaki gibi açın:



Şekil 4: Ayarlar – Kullanıcı Arayüzü Tercihleri bölümü

**5. Adım.** Yukarıdaki Şekil 4'te görüldüğü gibi aşağı açılır Dil menüsünü *bulun* ve istediğiniz dili **seçin**.

### 3.1 Sanal Klavye Nasıl Kullanılır?

Kamuya açık veya paylaşılan bir bilgisayar kullanıyorsanız (örneğin internet kafe, sosyal merkez veya kütüphanede), parolanızı **sanal klavye** kullanarak girebilirsiniz. Bu klavye *tuş-kaydedici* programlara karşı e-posta hesabınız için ek bir koruma sağlar. Tuş-kaydedici programlar, kullanıcının fiziksel tuş darbelerini gözetleyerek parolaları, kullanıcı adlarını ve diğer önemli bilgileri kaydetmek için kullanılır. Sanal klavye ise kullanıcının parolasını fare kullanarak girmesine izin vererek kullanıcıların bu güvenlik boşluğunu aşmalarını sağlar.

**RiseUp** sanal klavyesini kullanmak için aşağıdaki adımları takip ediniz:

**1. Adım.** RiseUp ana sayfasını **açın** <https://mail.riseup.net/> [84].

**2. Adım.** Sanal klavyeyi aşağıda görüldüğü gibi etkinleştirmek için 'yi **tıklayın**:



Şekil 5: Sanal klavye etkinleştirilmiş bir şekilde RiseUp Giriş sayfası

**3. Adım.** Parolanızı girmek için farenizi kullanarak ekranda görünen tuşlara **basın**. Sanal klavye için, klavyenin yukarı sol köşesindeki aşağı açılan menüden bir dil seçebilirsiniz. Sanal klavyedeki bazı karakterlere ulaşmak için 'Alt' ya da 'AltGr' tuşlarını kullanmanız gerekebilir.

**4. Adım.** RiseUp hesabınıza erişmek için 'i tıklayın.

## Hesap Ayarlarınızı Nasıl Değiştirebilirsiniz?

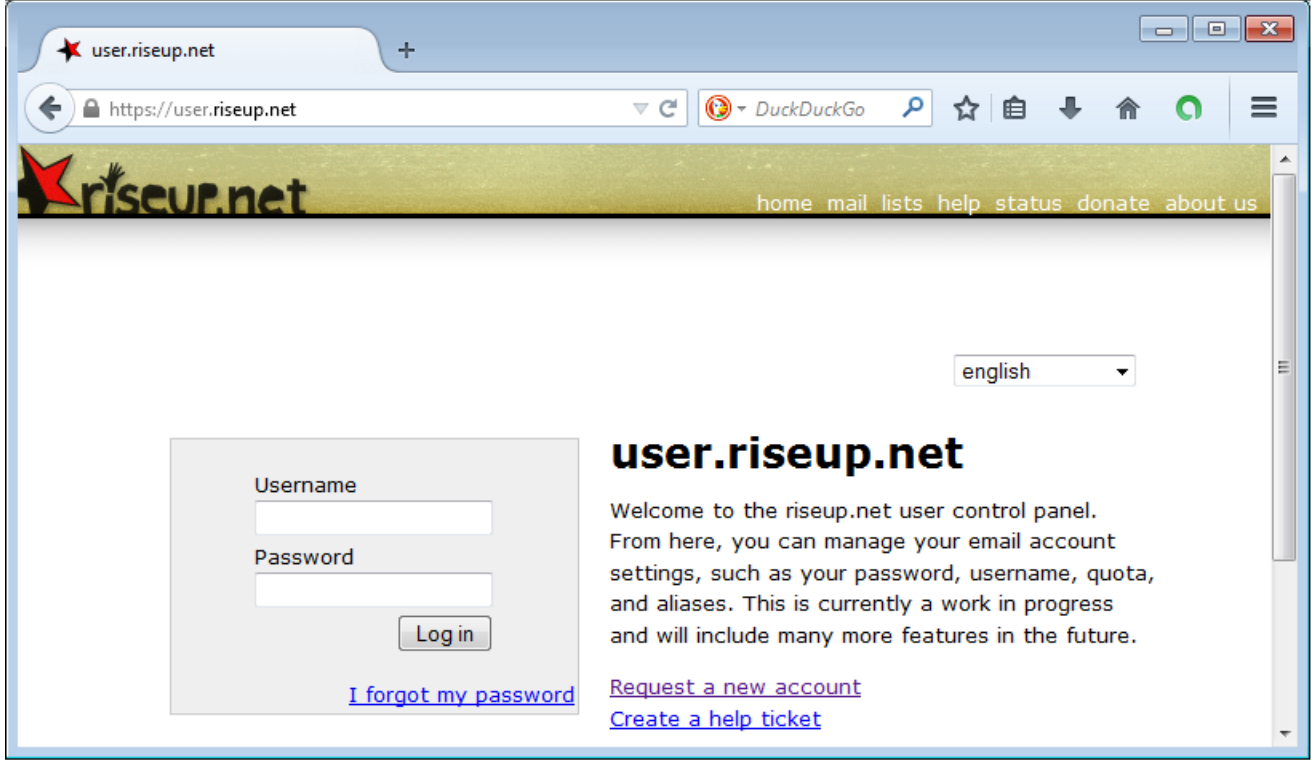
Bu sayfadaki kısımların listesi::

- [4.0 Hesap Ayarlarınızı Nasıl Deęiřtirebilirsiniz?](#)
- [4.1 Ayarlarım sayfası](#)
- [4.2 E-posta ayarları sayfası](#)
- [4.3 Davetler sayfası](#)

## 4.0 Hesap Ayarlarınızı Nasıl Deęiřtirebilirsiniz?

**RiseUp** hesabınız için çeřitli ayarlar seçmenize olanak verir. E-posta kutunuzun kapasitesini belirleyebilir, hesap adınızı ve adresinizi deęiřtirebilir, rumuz ekleyebilir ve daha birçok bařka iřlem yapabilirsiniz. Aynı zamanda, davet kodları yaratarak, arkadař ve meslektařlarınızın kendi **RiseUp** hesaplarını oluřturmalarına yardımcı olabilirsiniz.

**1. Adım.** **RiseUp** Hesap ayarları sayfasını ařaęıda görüldüęü gibi **açın**: <https://user.riseup.net/> <sup>[91]</sup>



řekil 1: user.riseup.net sayfası

**2. Adım.** Kullanıcı adınızı ve parolanızı ilgili alanlara **girin**.

**3. Adım.** Ařaęıda görünen ekranı açmak için 'i **tıklayın**:

 My Settings Email Help Tickets Invites Shell VPN Logout

## ssayyedd's home

Welcome to your user control panel. Eventually, this will be a central place for you to set preferences, get help, and request new services. Currently, the control panel only supports email preferences.



### Get Help

1. [Help with my email account »](#)
2. [Help with my mailing list »](#)
3. [Other help question »](#)



### Request new service

1. [Close my email account »](#)
2. More to come soon...

Şekil 2: riseup.net kullanıcı kontrol sayfası

#### 4.1 Ayarlarım sayfası

Ayarlarım sayfası **RiseUp Hesabı Oluştur** <sup>[95]</sup> sayfasında girdiğiniz bilgileri gösterir.

1. Adım. Aşağıda görünen ekranı açmak için  **My Settings** 'i tıklayın:

★ My Settings

Email

Help Tickets

Invites

Shell

VPN

Logout

## Settings for ssayedd

On this page, you may edit your general user settings, such as your username, p

### About Me

Username

ssayedd

To change your primary email address, you can account instead. WARNING: your account will b take a few minutes.

Alternate email

If you forget your password, you will be able to alternate email addresses to contact you when request has been processed. If you do not fill c password. You can specify more than one alter

### Password

Password

If you wish to change yo

Retype password

Retype your password to

### Locale

Language

english

This setting determines your default

Country

We use the country information to c servers. This information is entirely o

Time Zone

All times displayed in the user contr

Save Changes

Şekil 3: Ayarlar sayfası

Bu sayfada kullanıcı adınızı değiştirebilirsiniz, bu e-posta adresinizi de değiştirecektir. Yeni kullanıcı adı da emsalsiz olmalıdır. Bu sayfadan başka e-posta adresi, parola ve benzeri konularda da değişiklik yapabilirsiniz.

**Dikkat ederseniz,** *Dil*, *Ülke* ve *Zaman Dilimi* alanları değiştirilmemiş veya boş bırakılmıştır. Bunun sebebi sunucu üzerindeki kişisel bilgilerinizi mümkün mertebe azaltmaktır.

**2. Adım.** Yeni bilgilerinizi **girin** ve daha sonra aşağıdaki mesajı görmek için **Save Changes** 'i **tıklayın**:



Şekil 4: Değişiklikler başarı ile kaydedilmiştir

## 4.2 The Email settings page

The *Email settings* page lets you modify or view information related to email storage. You can even set the 'quota' or amount of space reserved for your email account on a **RiseUp** server.



**Step 1.** Click to open the following screen:

The screenshot shows the 'Email settings' page in the RiseUp.net user control panel. The page has a sidebar on the left with links to 'My Settings', 'Email', 'Help Tickets', 'Invites', 'Shell', 'VPN', and 'Logout'. The main content area is titled 'Email settings' and contains three tabs: 'My mailbox', 'Spam settings', and 'Mail filters'. Below the tabs, there is a text box stating: 'On this page, you may edit your preferences relating to email, such as your quota'. The settings are organized into a table-like structure with three columns: the setting name, the current value, and a description. The settings are: 'Address' (ssayyedd@riseup.net), 'Keep backups' (checked), 'Quota' (92 megabytes), and 'Storage host' (spoonbill-pn.riseup.net). Below this table is a section titled 'Aliases and forwarding' which contains two rows: 'Aliases' with a text input field containing 'safeandsecure' and 'salsaytester', and 'Forward' with an empty text input field. A 'Save Changes' button is located at the bottom of the settings area.

| Setting      | Value                               | Description            |
|--------------|-------------------------------------|------------------------|
| Address      | ssayyedd@riseup.net                 | This is y              |
| Keep backups | <input checked="" type="checkbox"/> | If check<br>eats all   |
| Quota        | 92 megabytes                        | You can<br>hardwar     |
| Storage host | spoonbill-pn.riseup.net             | This is tl<br>directly |

| Aliases and forwarding |                                                         |                                               |
|------------------------|---------------------------------------------------------|-----------------------------------------------|
| Aliases                | <input type="text" value="safeandsecure salsaytester"/> | Aliases a<br>address,<br>receiving<br>account |
| Forward                | <input type="text"/>                                    | Specify<br>forward                            |

Save Changes

Şekil 5: E-posta ayarları sayfası

**2. Adım.** Kota metin kutusuna uygun olan bir sayıyı **girin**.

**Not:** Hesabınızın kapasitesi disk kotanız ile sınırlıdır (şu anda bu kota verili olarak 92 mb'dir). Daha fazla alana ihtiyacınız varsa, e-postalarınızı Thunderbird gibi bir posta istemcisi kullanarak indirebilir ve e-postalarınızı sunucuda saklayabilirsiniz.

Bu sayfada hesabınız için rumuz da yaratabilirsiniz. Rumuz hesabınız için takma bir isim oluşturmak anlamına gelir. Ana hesapta bir değişiklik olmasa da insanlar rumuz adresinize de posta gönderebilir hale gelir.

This screenshot shows a close-up of the 'Aliases and forwarding' section. It has two rows. The first row is labeled 'Aliases' and has a text input field containing the text 'safeandsecure' and 'salsaytester' on two lines. The second row is labeled 'Forward' and has an empty text input field.

| Aliases and forwarding |                                                         |
|------------------------|---------------------------------------------------------|
| Aliases                | <input type="text" value="safeandsecure salsaytester"/> |
| Forward                | <input type="text"/>                                    |

Şekil 6: E-posta ayarlar sayfasındaki rumuz bölümü

Örnek: **ssayyedd@riseup.net** hesabının iki rumuzu var. **safeandsecure@riseup.net** ve **salsaytest@riseup.net** adreslerine gönderilen e-postalar ana hesaba aktarılacak. Bu yöntemle gerçek hesap adresinizi gizli tutabilirsiniz.

**Not:** Bu sayfada Şekil 5'te gösterilen sekmeler ve bağlantılar aracılığıyla erişebileceğiniz başka yapılandırma ayarları da vardır. Bunlardan bazıları:

- *İstenmeyen e-posta ayarları:* RiseUp sunucusunun istenilmediği düşünülen e-postaları nasıl ayarlayacağını yapılandırmanızı sağlar;
- *E-posta filtreleri:* RiseUp sunucusunun gelen e-postalarınızı farklı klasörlere koyması ya da belli e-postaları silmesi işlemlerini yapılandırmanızı sağlar;
- *Gelen kutusunu düzeltme:* Gelen kutusunun çalışmadığı durumlarda yardımcı olur;
- *E-postaları yedeklerden geri yükle:* Gelen kutusu içeriğinizi RiseUp sunucusu üzerinde saklanmış yedeklerden geri yüklemenizi sağlar;

- *Gelen kutusunu yok et:* Gelen kutunuzu, tüm kalsörlerdeki e-postalar ile birlikte, tamimiyle yok eder. Bu hesaba giriş yapmaya devam edebilirsiniz ve yeni (boş) bir gelen kutusu yaratabilirsiniz.

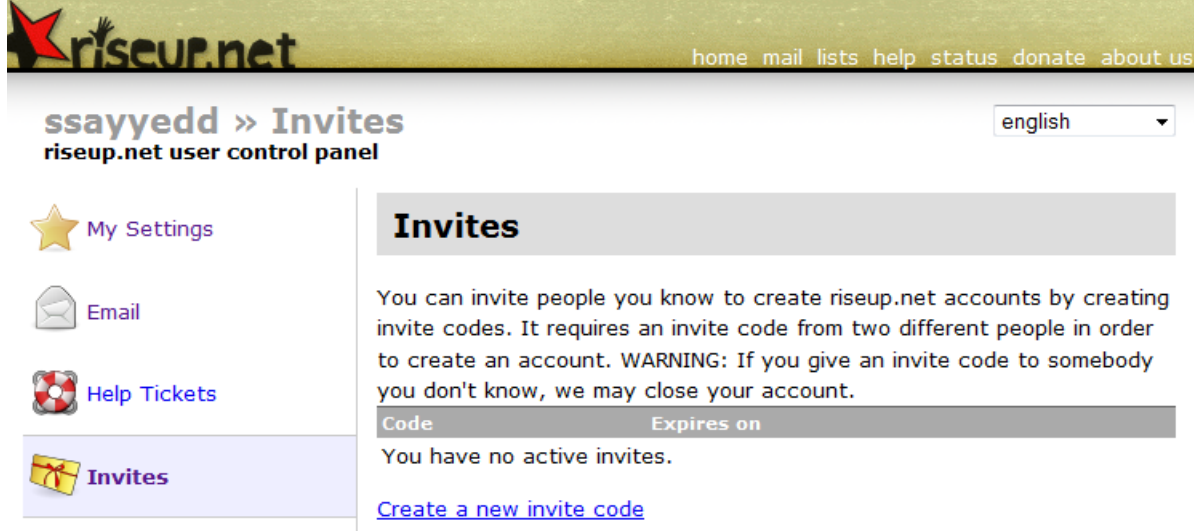
3. Adım. Yeni ayarlarınızı kaydetmek için 'ı tıklayın.

## 4.3 Davetler sayfası

*Davetler* sayfası, arkadaşlarınızı ve meslektaşlarınızı **RiseUp'a** katılmak için davet etmenizi mümkün kılan *davet kodları* oluşturmanızı sağlar.

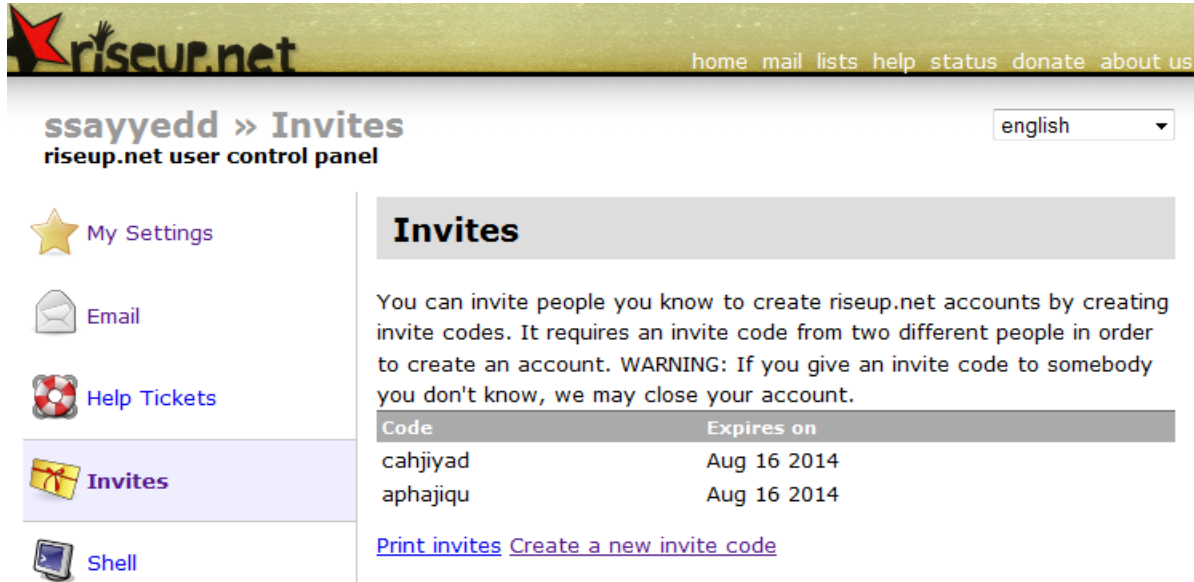
**Önemli:** Her yeni hesap iki farklı kullanıcıdan gelecek davet kodlarına ihtiyaç duyar. İstedığınız kadar davet kodu oluşturabilirsiniz.

1. Adım. Aşağıdaki ekranı etkinleştirmek için 'ı tıklayınız.



Şekil 7: Davetler sayfası

2. Adım. Davet kodlarını aşağıda görüldüğü gibi oluşturmak için [Create a new invite code](#) 'u tıklayın:



Şekil 8: Oluşturulmuş bir davet kodu örneği

**Not:** Her davetiye kodu bir ay süresince geçerlidir.

3. Adım. Davetiye kodlarının bir kopyasının çıktısını almak ve **RiseUp** hesabı açmak isteyen kişiye vermek için [Davetin Çıktısını Al](#) <sup>[96]</sup> 'ı tıklayın.

4. Adım. Kullanıcı bölmesinden çıkış yapmak için  Logout'u tıklayın.

# RiseUp - Sıkça Sorulan Sorular

## 5.0 Sıkça Sorulan Sorular

**Soru:** Riseup hesabıma giriş yapamıyorum.

**Cevap:** Lütfen Riseup E-posta Yardım <sup>[89]</sup> kısmındaki Web posta girişi sorunu giderme bölümüne <sup>[97]</sup> bakın. Diğer birçok konu için Riseup Yardım: Sıkça Sorulan Sorular'a bakabilirsiniz <sup>[98]</sup>.

**Soru:** Hangi durumlarda SquirrelMail web e-posta arayüzü yerine verili (Roundcube) kullanmalıyım?

**Cevap:** Eğer herhangi bir sebepten dolayı bir e-posta arayüzü çalışmazsa veya rutin bir bakım altındaysa, işleminizi kesintiye uğratmadan başka bir e-posta arayüzünü kullanmaya devam edebilirsiniz. Ayrıca, SquirrelMail servisi JavaScript gerektirmez.

**Soru:** Hesap oluştururken kendimle ilgili bilgi vermekten rahatsız oluyorum, bu bilgileri sağlamak zorunda mıyım?

**Cevap:** Hayır, istemediğiniz takdirde kişisel bilgi vermek zorunda değilsiniz.

**Soru:** Tanıdığım bir aktivist için nasıl e-posta hesabı oluşturabilirim?

**A:** Başka bir Riseup kullanıcısı ile birlikte davet kodu <sup>[80]</sup> oluşturmanız ve tanıdığınıza bunları göndermeniz gerekir. Söz konusu kişi Riseup hesabı oluşturmak istediğinde bu kodları kullanacaktır.

**Soru:** Roundcube web posta arayüzünde iki-faktörlü kimlik doğrulama olduğunu gördüm, onu kullanmalı mıyım?

**Cevap:** İki-faktörlü kimlik doğrulama giriş yaparken parolanıza ek olarak rastgele ve değişken bir kod girmenizi isteyerek e-posta hesabınıza ek bir koruma sağlar. Fakat, bunu kurup etkinleştirdikten bile SquirrelMail web e-posta arayüzü veya POP/IMAP erişimi üzerinden bir e-posta istemcisi ile (Thunderbird) iki-faktörlü kimlik doğrulamaya ihtiyaç duymadan e-postalarınıza ulaşmak mümkündür. Riseup servisinin iki-faktörlü kimlik doğrulama desteğini geliştirmesini sabırsızlıkla bekliyoruz.

## 5.1 Gözden Geçirme Soruları

- E-postanızı web posta üzerinden veya bir e-posta istemci programı ile okumanız arasındaki fark nedir?
- Güvenli Soket Katmanı (SSL) nedir ve nasıl çalışır?
- Sanal klavye nedir ve nasıl çalışır?
- E-posta hesabınıza nasıl rumuz eklersiniz?
- Yeni oluşturulmuş bir davetiye kodu ne kadar süre geçerlidir?

## Pidgin ve OTR- Güvenli Anlık Mesajlaşma

**Short Description:**

Pidgin ücretsiz ve açık kaynak olan, tek bir arayüz kullanarak farkı Anlık Mesajlaşma (Instant Messaging, IM) hesaplarınızı organize etmenizi ve yönetmenizi sağlayan bir istemcidir. Kendisi için tasarlanmış olan Off-the-Record (OTR) eklentisiyle beraber Pidgin, kullanıcıları arasında kimlik doğrulamalı ve güvenli bir iletişim temin eder.

**Online Installation Instructions:**

**Pidgin ve OTR'yi Kurma**

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki Pidgin ikonunu tıklayarak [www.pidgin.im/download/windows](http://www.pidgin.im/download/windows) sayfasını açın
- Windows için Pidgin'i indir linkini tıklayın
- Kurulum dosyasını bilgisayarınıza kaydedin, yerini bulup üstüne çift tıklayın
- Aşağıdaki OTR ikonuna tıklayarak <https://otr.cypherpunks.ca/index.php#downloads> sayfasını açın
- OTR plugin for Pidgin kısmında Win32 installer for pidgin 2.x linkini tıklayın
- Kurucuyu bilgisayarınıza kaydedin, yerini bulup üstüne çift tıklayın
- Pidgin ve OTR'yi başarıyla kurduktan sonra kurulum programlarını bilgisayarınızdan silebilirsiniz.

**Pidgin: OTR:**



<sup>[99]</sup>

Off-the-Record

<sup>[100]</sup>

**Ana Sayfa**

- Pidgin: [www.pidgin.im](http://www.pidgin.im) <sup>[101]</sup>
- OTR: <https://otr.cypherpunks.ca> <sup>[102]</sup>

## Bilgisayar Gereksinimleri

- İnternet bağlantısı
- Bütün Windows sürümleri

## Bu rehberde kullanılan sürümler

- Pidgin 2.10.9
- OTR 4.0.0-1

## Bu bölümün son güncellenme tarihi

- Ağustos 2014

## Lisans:

- Ücretsiz ve Açık-Kaynak Yazılım

## Gerekli Okuma

Nasıl Yapmalı Kitapçığının [7. Bölümü](#), [İnternet İletişiminizin Gizliliği Nasıl Korunur](#) <sup>[51]</sup>

## Buradan sağlayacağınız faydalar:

- En popüler anlık mesajlaşma servislerinden bazılarını tek bir program ile organize edip yönetebilme olanağı
- Özel ve kimlik denetimli sohbet edebilme olanağı

## GNU Linux, Mac ve Microsoft Windows'a Uyumlu Diğer Programlar

**Not:** Pidgin'e alternatif olarak [Jitsi'yi](#) <sup>[103]</sup> öneriyoruz. **Jitsi'yi** güvenli metin bazlı sohbetlerin yanında (ki bunu **Jitsi** üzerinden **Pidgin** kullanıcılarıyla da yapabilirsiniz), diğer **Jitsi** kullanıcılarıyla güvenli ses ve video iletişimleri kurmak için kullanabilirsiniz. **Jitsi Microsoft Windows, GNU/Linux, Mac OS** ve diğer işletim sistemleri için kullanıma açıktır.

Hem **Pidgin** hem de **OTR**; **Microsoft Windows** ve **GNU/Linux** için kullanıma açıktır. **OTR'yi** destekleyen **Microsoft Windows** için bir diğer anlık mesajlaşma programı da [Miranda IM'dir](#) <sup>[104]</sup>. **Mac OS** için **OTR** eklentisini destekleyen çok protokollü [Adium'u](#) <sup>[105]</sup> kullanabilirsiniz.

## 1.1 Başlamadan önce bu araç hakkında bilmeniz gerekenler

**Pidgin'i** kullanmaya başlamadan önce bir **anlık mesajlaşma** hesabınız olmalı, ancak bundan sonra o hesabı **Pidgin'e** kaydedebilirsiniz. Örnek olarak, bir **Google** hesabınız varsa, onların **anlık mesajlaşma** servisi **GoogleTalk'ı** **Pidgin** ile kullanabilirsiniz. Varolan **anlık mesajlaşma** hesabınızın giriş detayları hesabınıza **Pidgin** aracılığıyla ulaşabilmek için kullanılır.

**Not:** Bütün kullanıcılar **Anlık Mesajlaşma hesabı sağlayıcılarının** gizlilik ve güvenlik politikaları hakkında mümkün olduğunca bilgi edinmeye teşvik edilir.

**Pidgin** şu **anlık mesajlaşma** servislerini destekler: **AIM** <sup>[106]</sup>, **Bonjour** <sup>[107]</sup>, **Gadu-Gadu** <sup>[108]</sup>, **Google Talk** <sup>[109]</sup>, **Groupwise**, **ICQ** <sup>[110]</sup>, **IRC**, **MSN** <sup>[111]</sup>, **MXit** <sup>[112]</sup>, **MySpacelM** <sup>[113]</sup>, **SILC** <sup>[114]</sup>, **SIMPLE**, **Sametime** <sup>[115]</sup>, **Yahoo!** <sup>[116]</sup>, **Zephyr** ve **XMPP** mesajlaşma protokolünü takip eden bütün **anlık mesajlaşma** istemcileri.

**Pidgin** değişik **anlık mesajlaşma** servisleri arasında iletişime izin vermez. Örnek olarak siz **Pidgin'i** **GoogleTalk** hesabınıza ulaşmak için kullanıyorsanız, **ICQ** hesabını kullanan bir arkadaşınızla sohbet etmeniz mümkün değildir.

Yine de, **Pidgin** desteklediği bütün mesajlaşma protolleri üstünden çalışan hesaplarınızın hepsini birden yönetmeniz için yapılandırılabilir. Böylece, hem **Gmail** hem de **ICQ** hesabınızı aynı anda kullanabilir, ve arkadaşlarınızla bunlardan **biri** aracılığıyla (çünkü ikisi de **Pidgin** tarafından desteklenir) sohbet edebilirsiniz.

**Off-the Record (OTR)** mesajlaşma özellikle **Pidgin** için geliştirilmiş bir eklentidir. Aşağıdaki gizlilik ve güvenlik özelliklerini kullanımınıza sunar:

- **Kimlik Denetleme:** İrtibatta olduğunuz kimsenin kimliğinden hep emin olursunuz.
- **İnkâr Edebilme:** Sohbet oturumu bittikten sonra, mesajlarınızın sizden ya da irtibatta bulunduğunuz kişiden kaynaklandığı gösterilemez.
- **Şifreleme:** Sizden başka kimse anlık mesajlarınıza ulaşamaz ya da onları okuyamaz.
- **Mükemmel İleri Yönlendirme Güvenliği:** Üçüncü şahıslar özel anahtarlarınızı ele geçirecek dahi olsa, eski sohbetlerinizden hiçbirisi tehlike altında değildir.

**Not:** **OTR** eklentisinden önce **Pidgin** indirilmelidir.

## Offline Installation Instructions :

## OTR ile Pidgin'i Kurma

- *Kısa Uygulamalı Rehberler'in* <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **OTR ile Pidgin** ikonunu **tıklayın** ve kurucuyu 'Açın' ya da 'Çalıştırın'. Gerekirse, önce kurucuyu kaydedin, sonra kaydettiğiniz yeri bulup üstüne çift tıklayın
- Devam etmeden önce bir sonraki kısımdaki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz, kurulumdan sonra silebilirsiniz

Pidgin: OTR:



[117]

Off-the-Record

[118]

## Pidgin ve OTR yazılımlarını Nasıl Kurabilir ve sonrasında Hesabınızı Pidgin'e Nasıl Kaydedebilirsiniz?

Bu sayfadaki kısımların listesi:

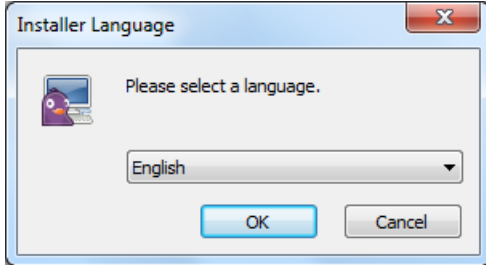
- **2.0 Pidgin Hakkında**
- **2.1 Pidgin Nasıl Kurulur?**
- **2.2 Off-The-Record (O) Eklentisi Nasıl Kurulur?**
- **2.3 Pidginde Hesap Kaydı ve Kurulumunu İşlemine Genel bir Bakış**
- **2.4 Anlık Mesajlaşma Hesabınız Pidgin'e Nasıl Kaydedilir?**
- **2.5 Pidgin'de Arkadaşlar Nasıl Eklenir?**
- **2.6 Pidgin'de Anlık Mesajlaşma Penceresi Nasıl Açılır?**
- **2.7 Pidgin'de bir Hesap Nasıl Yeniden Etkinleştirilir?**

### Pidgin Hakkında

Hem **Pidgin** hem de onla ilintili otomatik şifreleme ve kimlik denetimi eklentisi olan **Off-the-Record'un (O)** çalışabilmesi için ikisinin de kurulması gereklidir. Neyse ki her iki programın da kurulum işlemi basit ve hızlıdır.

### 2.1 Pidgin Nasıl Kurulur?

**1. Adım.** pidgin-2.10.9.exe'ye **çift tıklayın**; Dosyayı Aç – Güvenlik Uyarısı kutusu açılırsa **Çalıştır** 'ı **tıklayarak** aşağıdaki ekranı görüntüleyin:



Şekil 1: Kurucu Dili onaylaması kutusu

**2. Adım.** 'ı **tıklayarak** Pidgin 2.10.9 Kurulum Sihirbazına Hoşgeldiniz ekranını açın.

**3. Adım.** 'ı **tıklayarak** Lisans Anlaşması ekranını açın; Lisans Anlaşması'nı okuduktan sonra 'ı **tıklayarak** Pidgin 2.10.9 Kurulumu – Bileşenleri Seçin ekranını açın.

**4. Adım.** 'ı **tıklayarak** Pidgin 2.10.9 Kurulumu – Kurulum Yerini Seçin penceresini açın.

**5. Adım** 'ı **tıklayarak** verili kurulum dizinini kabul edin ve **Pidgin** yazılımını kurmak üzere Pidgin 2.10.9 Kurulumu – Kuruluyor penceresini açın.

Bir miktar klasör ve dosya sırayla hızlıca kurulacak; kurulum işlemi bitince Pidgin 2.10.9 Kurulumu –Kurulum Tamamlandı penceresi belirecek.

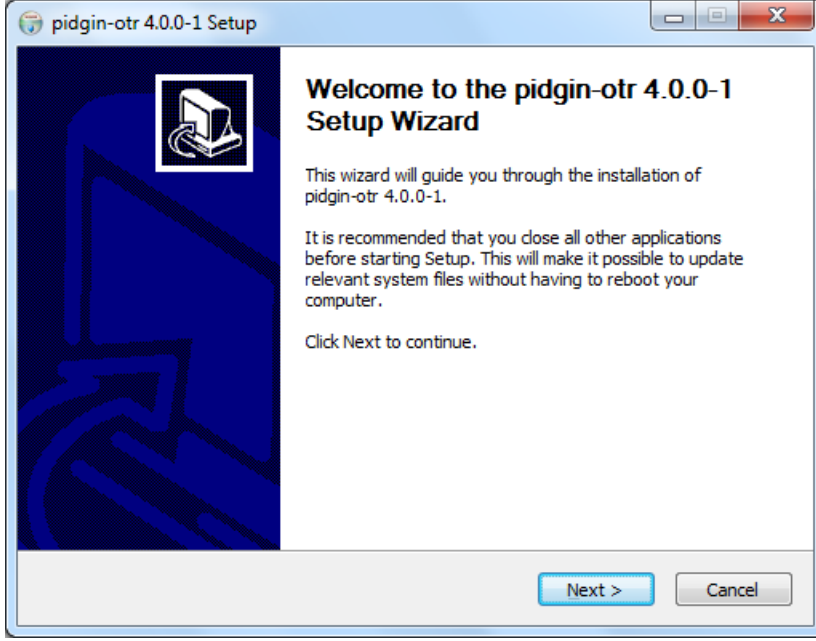
**6. Adım.** 'ı **tıklayarak** Pidgin 2.10.9 Kurulum Sihirbazı Tamamlanıyor'u görün.

**Not:** Kurulum işleminin **3. adımında Pidgin Başlangıç> Programlar** listesinde bulunacak şekilde yapılandırıldı, ve ileride buradan da başlatılabilir.

**7. Adım.** 'ı **tıklayarak** Pidgin'in kurulumunu tamamlayın.

## 2.2 Off-The-Record (O) Eklentisi Nasıl Kurulur?

1. Adım.  'ye çift tıklayın; Dosyayı Aç – Güvenlik Uyarısı kutusu açılırsa **Çalıştır** 'ı tıklayarak aşağıdaki ekranı görüntüleyin:



Şekil 2: Pidgin-o 4.0.0-1 Kurulum Sihirbazına Hoşgeldiniz ekranı

2. Adım.  'ı tıklayarak *Lisans Anlaşması* ekranını görün; *Lisans Anlaşması* 'nı okuduktan sonra  'ı tıklayarak *Pidgin-o 4.0.0-1 Kurulumu – Kurulum Yerini Seçin* ekranını görüntüleyin.

3. Adım.  'ı tıklayarak kurulum işlemini başlatın.

4. Adım.  'ı tıklayarak **Pidgin-O** mesajlaşma yazılımı eklentisinin kurulumunu tamamlayın.

**Pidgin** ve **O** 'nin kurulumunu tamamladığınızda ve **Pidgin** 'i **Başlangıç>Programlar** listesinden başlattığınızda, Windows görev çubuğunda şu ikon belirecek:



Şekil 3: Siyahla çerçevelenmiş Pidgin-O ikonu

Tebrikler! **Pidgin** ve **O** programlarını kurmayı başarı ile tamamladınız!

## 2.3 Pidginde Hesap Kaydı ve Kurulumunu İşlemine Genel bir Bakış

**Pidgin** 'de hesap kaydı ve kurulumu işleminde dört temel adım vardır; varolan bir **anlık mesajlaşma** hesabını **Pidgin** 'e kaydetme, bir *irtibatı ekleme*, irtibatınızın da aynısını yapmasını sağlama, ve son olarak ilk sohbet seansınız için sohbet penceresine ulaşma.

Sohbet ya da **anlık mesajlaşma** oturumlarının iki katılımcı arasında yer aldığı için, buradaki örnekler değişik formatların ya da pencerelerin **her iki** katılımcıya (Salima ve Terence adında kurgusal karakterlerle temsil edilirler) hesap kaydı ve kurulumu işlemi esnasında nasıl görüneceği belirtecek. Bütün örnekler **Riseup.Net** anlık mesajlaşma servisine dayanır.

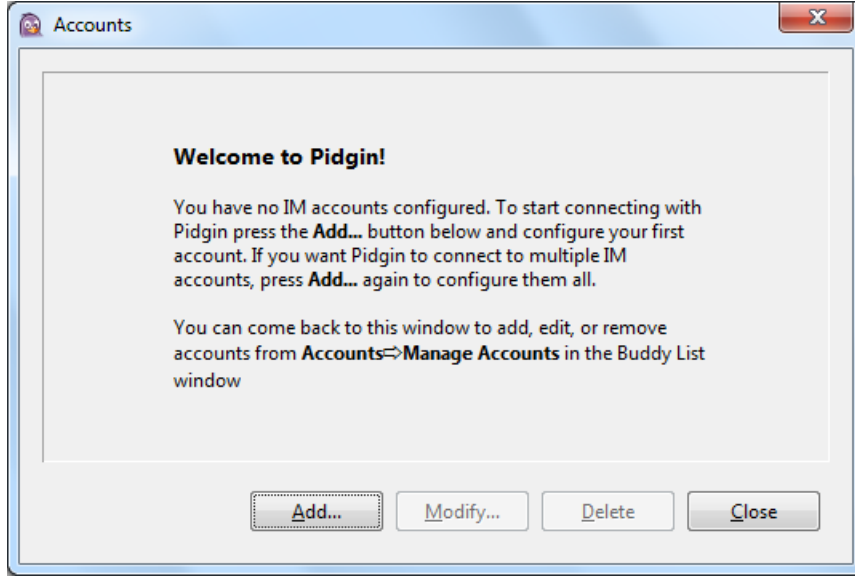
**Not:** **Pidgin** 'i kullanabilmeniz için, aşağıdaki *Şekil 6* 'da listelenmiş sağlayıcılardan bir tanesinden bir **Anlık Mesajlaşma (IM)** hesabınızın olması gerekir. Yeni bir **anlık mesajlaşma** hesabı kurmak isterseniz, [XMPP iletişimi](#) <sup>[76]</sup> için kullanılacak olan **Riseup.net** e-posta hesabını kullanmanızı öneririz. Lütfen **Riseup – Güvenli Email Servisi** <sup>[119]</sup> bölümüne daha fazla bilgi ve **Riseup** e-posta hesabını nasıl kuracağınıza dair yönergeler için bakın. Aynı zamanda [2.2. Jitside Hesaplar Nasıl Eklenir?](#) <sup>[120]</sup> kısmında listelenmiş [Jit.si](#) <sup>[121]</sup> ya da Google Hesabı gibi gibi XMPP hesabı sağlayıcılarını da kullanabilirsiniz.

## 2.4 Anlık Mesajlaşma Hesabınız Pidgin'e Nasıl Kaydedilir?

*Anlık mesajlaşma* hesabınızı **Pidgin** 'e kaydetmek için aşağıdaki adımları takip ediniz:

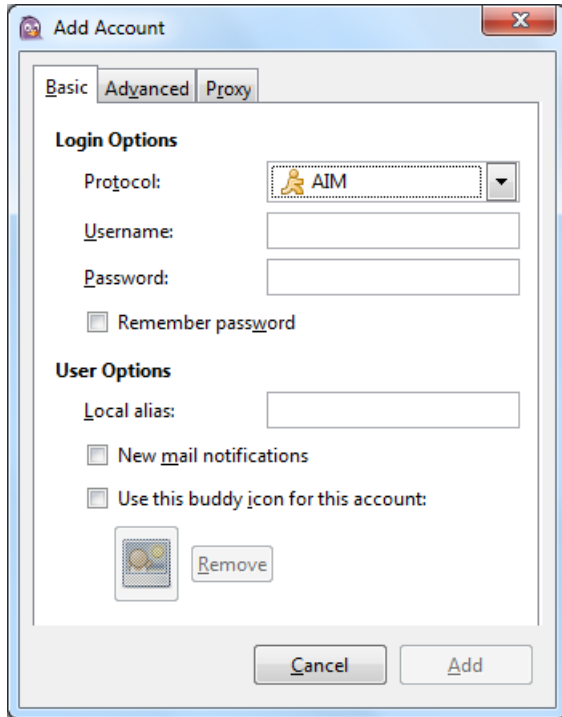


**1. Adım.** Pidgin'i **tıklayarak** ya da **Başlangıç > Programlar > Pidgin**'i seçerek **Pidgin**'i açın. **Pidgin**'i ilk defa açtığınızda aşağıdaki ekran belirir:



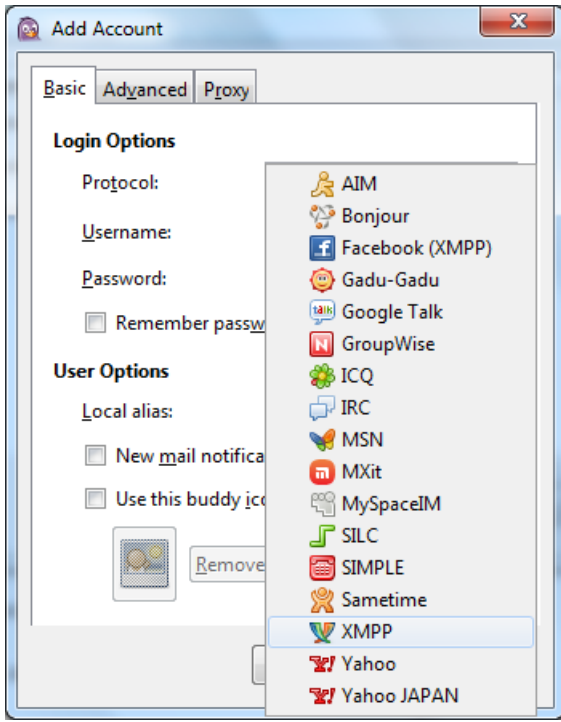
Şekil 4: Hesapları onaylama penceresi

**2. Adım.** **Add...** butonunu **tıklayarak** aşağıdaki gibi boş bir **Hesap Ekle** penceresi açın:



Şekil 5: Temel, Gelişmiş ve Proxy sekmeleri görünen Hesap Ekle ekranı

**3. Adım.** **Protokol** aşağı açılır listesini tıklayarak aşağıdaki gibi **Pidgin** tarafından desteklenen **anlık mesajlaşma** servisi protokollerini görünüz:



Şekil 6: Desteklenen anlık mesajlaşma protokollerini gösteren Hesap Ekle penceresi

**4. Adım.** Uygun olan **anlık mesajlaşma** protokolünü **seçin**.

**Not:** Her **anlık mesajlaşma** servisi sağlayıcısı için doldurmanız gereken girdi kutucukları farklı olacak. Fakat hepsi kesinlikle bir kullanıcı adı ve parola girmenizi isteyecek.

**5. Adım.** *Kullanıcı Adı* kutusuna e-posta adresinizi girin (mesela, [terencethetester@riseup.net](mailto:terencethetester@riseup.net) <sup>[122]</sup>).

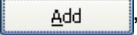
**6. Adım.** Bu hesapla ilgili olan parolanızı *Parola* kutusuna **girin**.

**7. Adım.** *Yerel Takma İsim* kutusuna dilediğiniz bir takma ismi **girin**. (Bu kutuyu doldurmak zorunlu değildir.)

**Önemli:** Gizlilik ve güvenliğinizi olabildiğince arttırabilmek için, *Parolayı hatırla* seçeneğini *etkinleştirmeyin*. Bu haliyle, **Pidgin** çevrimiçi sohbetlere ne zaman bağlanmak isterseniz sizi parolanızı girmeye davet edecek. Böylece başkalarının bilgisayarınızın başında beklemediğiniz anda **Pidgin'e** sizin adınıza bağlanmasını engellemiş olursunuz. Aynı zamanda, sohbet oturumunuz bittiğinde Arkadaşlar aşağı açılır menüsünden **Çık'ı seçmeyi** unutmayın!

Tamamlanmış bir *Hesap Ekle* ekranı aşağıdakine benzer:

Şekil 7: Tamamlanmış bir Hesap Ekle formu örneği

**8. Adım.** 'ı **tıklayarak** hesabınızı eklemeyi tamamlayın ve aynı anda güncellenmiş *Hesaplar* ve *Arkadaş Listesi* ekranlarını aşağıdakiler gibi görün:

Şekil 8: Güncellenmiş Hesaplar Penceresi; Şekil 9: Etkin moddaki Arkadaşlar Listesi

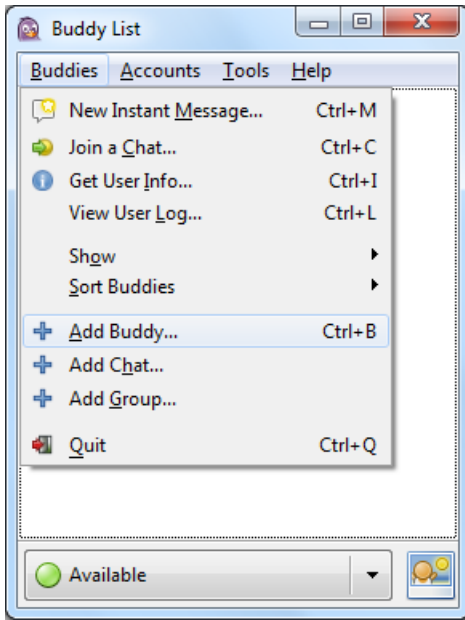
Bu adımları tamamladıktan sonra, artık *Pidgin* arkadaşlarınızı eklemeye ve onların irtibat bilgilerini girmeye hazırsınız.

## 2.5 Pidgin'de Arkadaşlar Nasıl Eklenir?

**Pidgin'de** arkadaşlarınız ya da irtibatlarınızı eklemek, onların irtibat detaylarını eklemek ve kaydetmeyi içerir. Takip eden örnekte Terence Salima'yı arkadaşı olarak ekliyor.

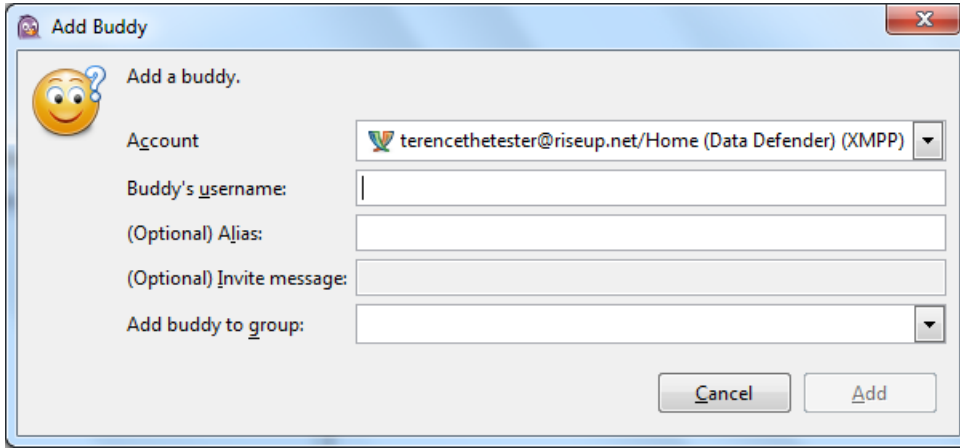
**Pidgin'de anlık mesajlaşma** hesabınıza bir arkadaş eklemek için aşağıdaki adımları takip edin:

**1. Adım.** *Arkadaşlar*'ı **tıklayarak** ilgili menüyü açın ve sonra *+ Arkadaş Ekle...*'yi aşağıdaki gibi **seçin**:



Şekil 10: 'Arkadaş Ekle...' öğesi seçilmiş Arkadaş Listesi menüsü

Bu aşağıdaki ekranı açacaktır:



Şekil 11: Arkadaş Ekle penceresi

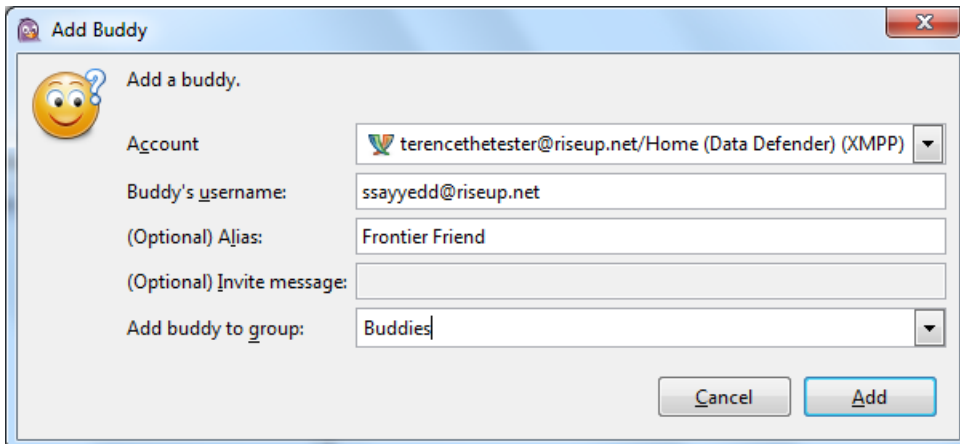
**2. Adım.** Birden fazla hesabınız varsa, 'arkadaşınızla' aynı mesajlaşma servisiyle alakalı olan hesabınızı **seçin**.

**Not:** Sizin ve arkadaşınızın **aynı** mesajlaşma servisini kullanıyor olması **gerekir**, o **Pidgin** kullanmıyor olsa bile. **Google Talk** hesabınıza bir **ICQ** ya da **MSN** arkadaşı ekleyemezsiniz. Fakat bu desteklenen protokollere bağlı birden fazla hesabı **Pidgin'de** kaydedip kullanabilirsiniz. Böylece **XMPP** hesabınızla bir arkadaşınızla sohbet ederken bir diğeriyle **ICQ** ya da **MSN** hesabınızı kullanarak sohbet edebilirsiniz.

**3. Adım.** *Kullanıcı Adı* kutusuna arkadaşınızın e-posta adresini **girin**.

Bir sonraki adım zorunlu değildir.

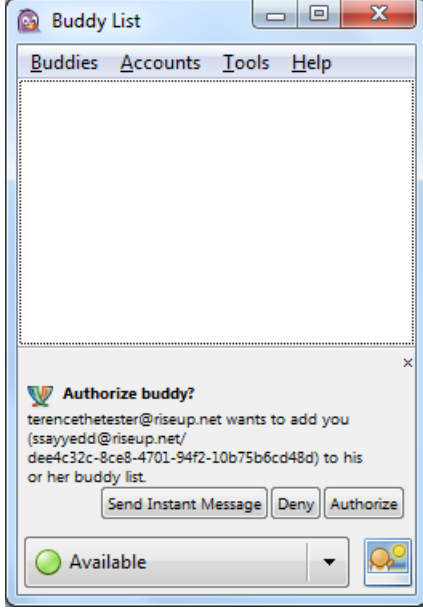
**4. Adım.** *Takma İsim* kutusuna bir *takma isim* **girin** ve *Arkadaş Ekle* formunuz aşağıdaki ekrana benzesin:



Şekil 12: Tamamlanmış bir Arkadaş Ekle formu örneği

5. Adım. **Add** i tıklayarak arkadaşınızı ekleyin.

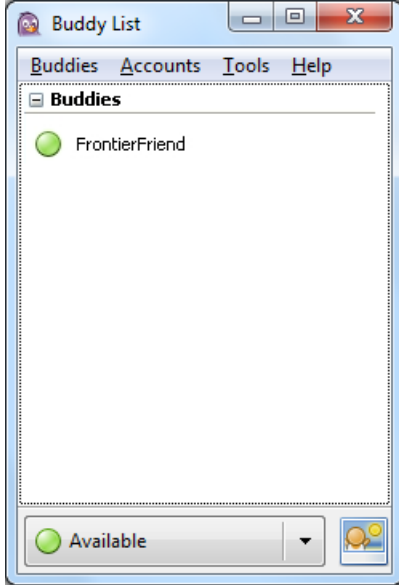
**Not:** Bu arkadaşınıza talebinizin onayı ya da iznini isteyen bir mesaj yollayacak ve arkadaşınızın Arkadaş Listesi'nde aşağıdaki gibi belirecek:



Şekil 13: Salima'nın Arkadaş Listesi'nde görüldüğü üzere arkadaşını Onayla talebi

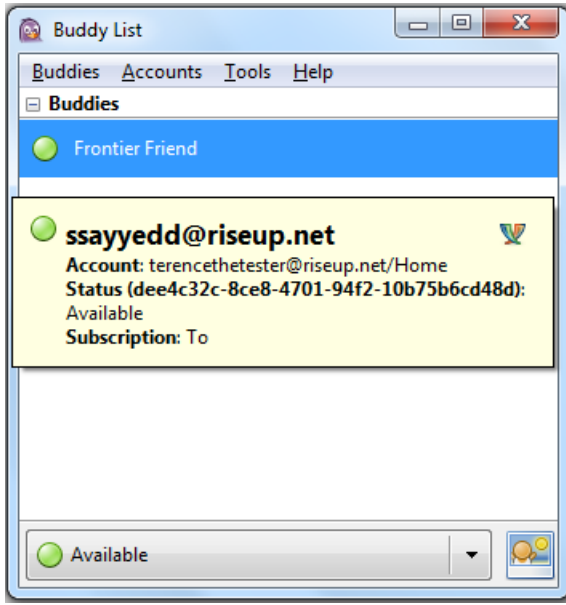
Bu noktada, arkadaşınız şu adımı uygulamalı:

6. Adım: **Authorize** i tıklayarak bu kişiyi arkadaşınız olarak ekleyin ve aşağıdaki gibi Arkadaş Listesi'nde görün:



Şekil 14: Salima'yı arkadaş olarak gösteren Terence'in Arkadaş Listesi

**Not:** Yukarıdaki örnekte, Salima'nın Takma Adı gösterilmektedir, bu da kimlik korunmasını bir kat daha güçlendirir.



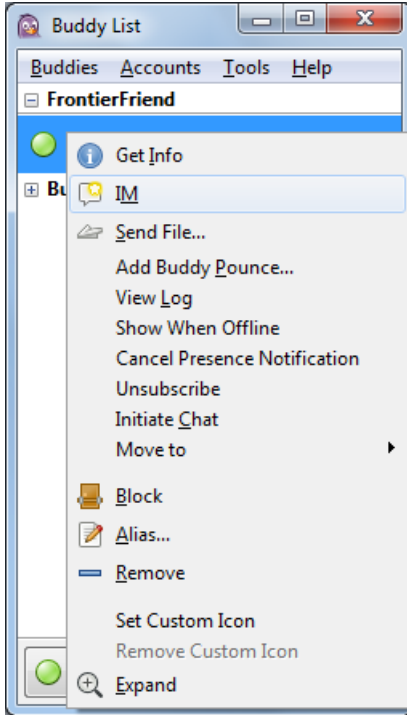
Şekil 15: Terence'in Salima'yı yeni eklenmiş arkadaşı olarak gösteren Arkadaş Listesi

**Pidgin** sohbet arkadaşınızı ekleyip, kimliğini doğrulayıp teyit ettikten sonra, onun da kendi hesabından sizin anlık mesajlaşma iletişim bilgilerini girmesi **1'den 6'ya** kadarki adımları takip etmesi gerekecek.

## 2.6 Pidgin'de Anlık Mesajlaşma Penceresi Nasıl Açılır?

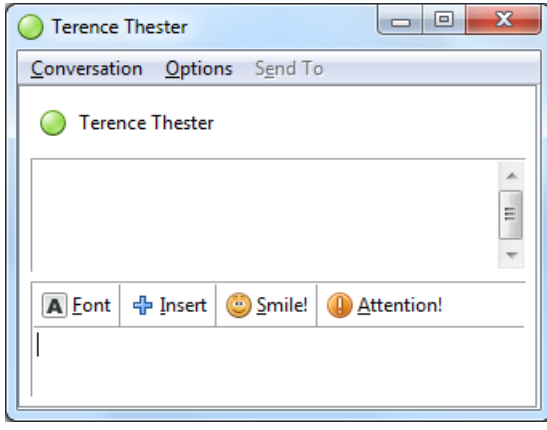
**Pidgin'de** bir **anlık mesajlaşma** penceresi açmak için aşağıdaki adımları takip edin:

**1. Adım.** Arkadaş listesinde bir arkadaşınızın adını **sağ tıklayarak** yapabileceğiniz bütün işlemleri gösteren menüyü aşağıda görüldüğü gibi açın:



Şekil 16: Arkadaş İşlemleri menüsü

**2. Adım.** Açılan menüde **Anlık Mesajlaşma'yı seçerek** tipik bir sohbet penceresini aşağıda gösterildiği gibi açın:



Şekil 17: Pidgin'de tipik bir sohbet penceresi

Şimdi arkadaşınızla **Pidgin**'i kullanarak sohbet etmeye neredeyse hazırsınız. Ama önce sohbet oturumunuzun özel ve güvenli olduğundan emin olmak için **O** şifrelemesini yapılandırmanız gerek. Bunun için bir sonraki sayfaya bakın.

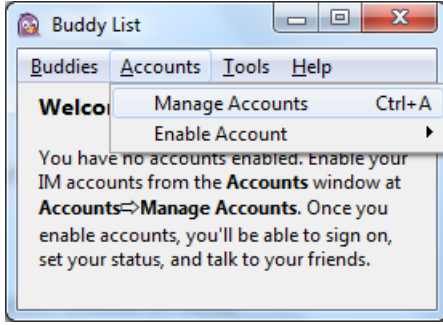
## 2.7 Pidgin'de bir Hesap Nasıl Yeniden Etkinleştirilir?

Zaman zaman anlık mesajlaşma hesabınızın **Pidgin**'de kendi kendine kapandığını fark edebilirsiniz; belki **Pidgin** programı internet bağlantısının kesilmesi nedeniyle uygun olmayan bir şekilde kapandığı için, ya da bilgisayarınız donduğu için. Neyse ki **Pidgin** hesabınızı tekrar etkinleştirmenin bir yolunu sunuyor. Bunun için aşağıdaki adımları takip edin:



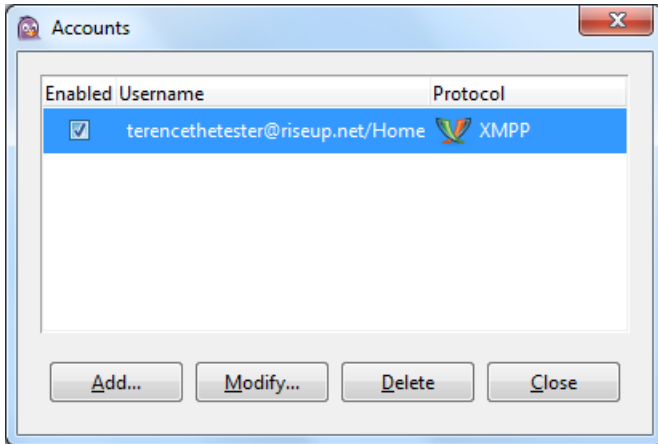
**1. Adım.** Pidgin 'i tıklayarak ya da **Başlangıç > Pidgin**'i seçerek Pidgin'i açın.

**2. Adım.** Hesaplar menüsünü **açın** ve sonrasında aşağıda gösterildiği gibi **Hesap Yönetimi** maddesini **seçin**:



Şekil 18: Hesap Yönetimi maddesi seçilmiş (boyutu değiştirilmiş) Hesaplar menüsü

Bu aşağıdaki ekranı açacak:



19. Şekil: Artık etkin olmayan bir hesabı gösteren Hesaplar penceresi (boyutu değiştirilmiş)

**3. Adım.** Hesabınızın yanındaki kutuyu **işaretleyerek Pidgin** parola sorgulamasını aşağıdaki gibi etkinleştirin:

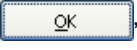


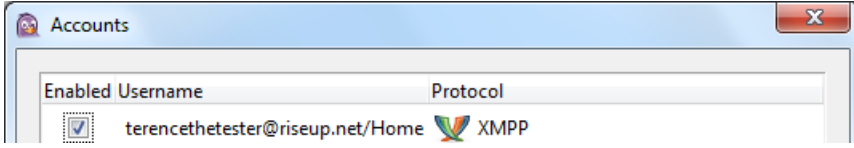
Şekil 20: Pidgin parola sorgulama kutusu

4. Adım. Parolanızı **girin** ve **Pidgin** parola sorgulama kutusu aşağıdakine benzesin:

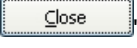


21. Şekil: Parola kutusu doldurulmuş Pidgin parola sorgulama kutusu

5. Adım. 'ı tıklayarak hesabınızı tekrar etkinleştirmeyi aşağıda görüldüğü gibi sonlandırın



Şekil 22: Başarıyla yeniden etkinleştirilmiş bir hesap

6. Adım. 'u tıklayarak Hesaplar penceresini kapatın.

## Pidgin'de OTR'yi Kullanarak Güvenli bir Mesajlaşma Oturumu Nasıl Açılır?

Bu sayfadaki kısımların listesi:

- **3.0 Pidgin ve OTR Hakkında**
- **3.1 Pidgin-OTR Eklentisi Nasıl Yapılandırılır?**
- **3.2 İlk Adım – Bir Özel Anahtar Nasıl Oluşturulur ve Parmak İzi Nasıl Görüntülenir?**
- **3.3 İkinci Adım – Bir Mesajlaşma Oturumu Nasıl Onaylanır?**
- **3.4 Üçüncü Adım – İrtibatta Olduğunuz Kişinin Kimliği Nasıl Teyit Edilir?**

### 3.0 Pidgin ve OTR Hakkında

Gizli ve güvenli **Anlık Mesajlaşma** oturumları açabilmeniz için hem sizin hem de irtibatta olduğunuz kişinin **OTR** eklentisini yapılandırması gerekir. **OTR** eklentisi her iki katılımcının da uygun bir şekilde bu eklentiye yükleyip yapılandırdığını otomatik olarak saptar.

**Not:** **OTR'yi** kurmamış ya da yapılandırmamış olduğunuz bir arkadaşınıza özel bir sohbet talebinde bulunursanız, otomatik olarak **OTR'yi** nereden bulabileceğini açıklayan bir mesaj yollar.

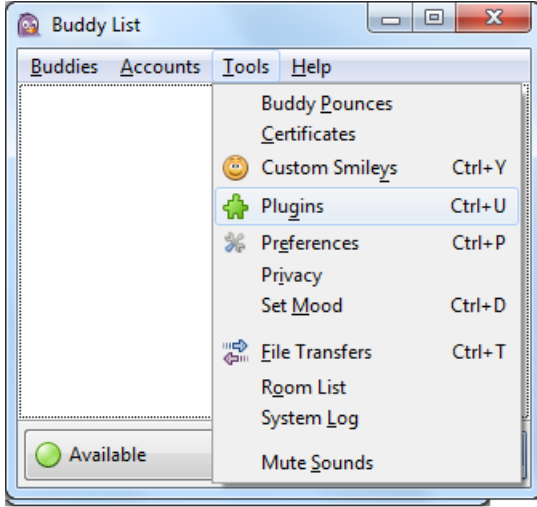
### 3.1 Pidgin-OTR Eklentisi Nasıl Yapılandırılır?

**OTR** eklentisini etkinleştirmek için aşağıdaki adımları takip edin:



**1. Adım.** Pidgin'e **çift tıklayarak**, ya da **Başlangıç > Programlar > Pidgin'i** seçerek **Pidgin'i** ve **Arkadaş Listesi** penceresini açın (Lütfen Şekil 1'e bakın).

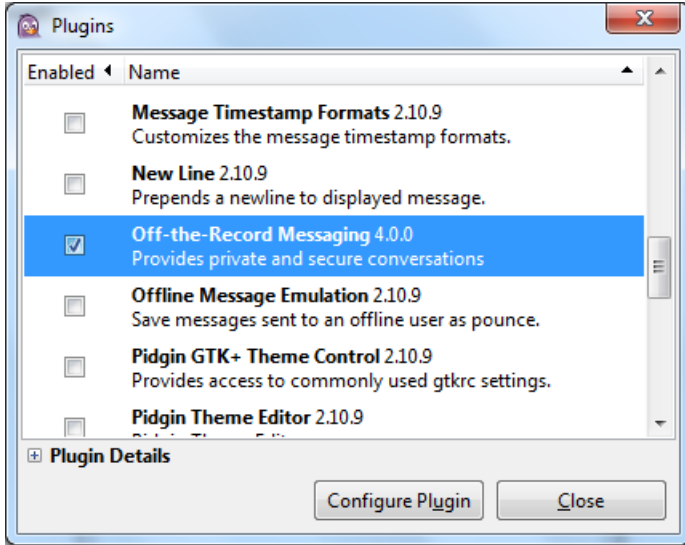
**2. Adım.** **Araçlar** menüsünü **Açın** ve sonrasında **Eklentiler** öğesini aşağıdaki gibi **seçin**:



Şekil 1: Araçlar menüsünden Eklentiler öğesi seçilmiş Arkadaş Listesi penceresi

Bu Eklentiler penceresini aşağıdaki gibi açacak:

**3. Adım.** Pencereyi *Off-the-Record Messaging*'a doğru **aşağı kaydırın**, sonrasında ilintili kutuyu **işaretleyin**.



Şekil 2: Off-The-Record Messaging'in seçili olduğu Pidgin Eklentiler penceresi

**4. Adım.** **Configure Plugin** i **tıklayarak** *Off-the-Record Mesajlaşma* pencerelerini yapılandırmaya başlayın.

Etkin bir şekilde özel ve güvenli **anlık mesajlaşma** oturumları açabilmek için **OTR'nin** yapılandırılmasının temelde 3 adımı vardır, ve bunlar aşağıda açıklanmıştır.

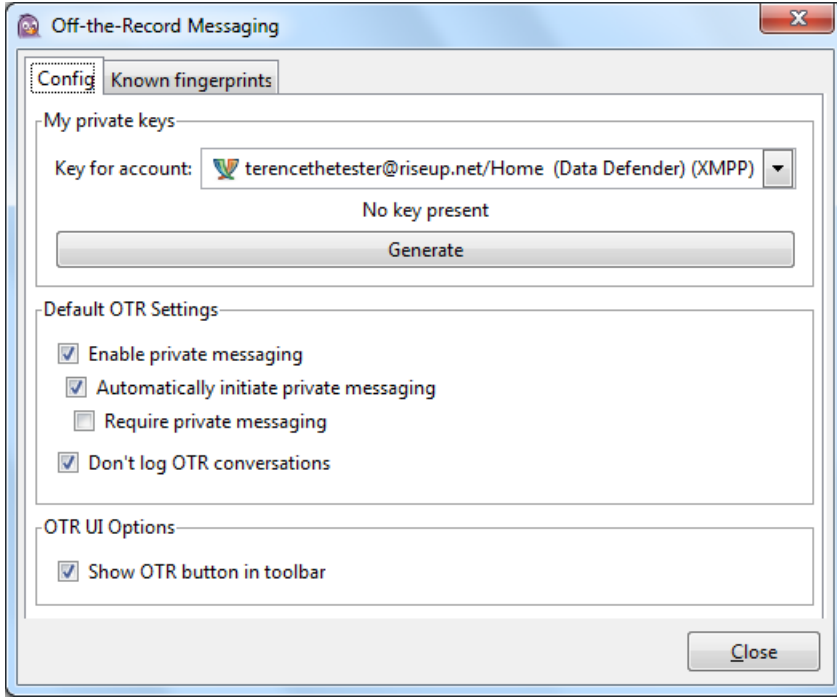
- **Birinci Adım:** Bu hesabınıza özgün bir özel anahtar oluşturmayı ve onun parmak izini görüntülemeyi içerir.

Bir sonraki adımlar *anlık mesajlaşma* oturumunu güvenlik altına almayı ve arkadaşlarınızın kimliğini doğrulamayı içerir..

- **İkinci Adım:** Bu bir katılımcının o anda çevrimiçi olan diğer katılımcıya özel ve güvenli bir sohbet oturumu açma talebini içerir.
- **Üçüncü adım Pidgin arkadaşınızın kimliğini doğrulamayı** içerir. (**Not: Pidgin'de, anlık mesajlaşma** oturumlarıyla irtibat kurmaya çalıştığınız herkes bir arkadaşdır.) Bir arkadaşın kimliğini doğrulamaya **Pidgin'de kimlik doğrulama** denir. Bu arkadaşınızın **kesinlikle** iddia ettiği kişi olduğunu tesbit etmek demektir.

## 3.2 İlk Adım – Bir Özel Anahtar Nasıl Oluşturulur ve Parmak izi nasıl Görüntülenir?

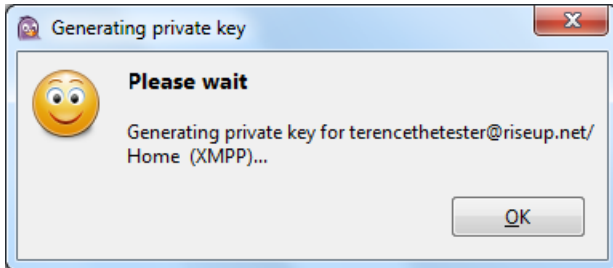
**Pidgin'de** güvenli sohbet oturumları ilgili hesap için bir *özel anahtar* oluşturmakla etkinleştirilebilir. *Off-the-Record* yapılandırma penceresi *Yapılandırma* ve *Tanınan parmak izleri* sekmeleriyle ayrılmıştır. *Yapılandırma* sekmesi her bir hesap için bir *özel anahtar* oluşturmak için ve belirli *OTR* seçeneklerini ayarlamak için kullanılır. *Tanınan parmak izleri* sekmesi irtibat kurduğunuz kişilerin parmak izlerinin bir listesini barındırır. Özel bir sohbet yapmak istediğiniz her bir arkadaşınız için bir anahtarınız olmalı.



Şekil 3: Yapılandırma sekmesi açılmış Off-the-Record Mesajlaşma ekranı

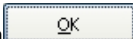
**1. Adım.** Gizliliğinizi olabildiğince artırmak için *Gizli mesajlaşmayı etkinleştirin*, *gizli mesajlaşmayı otomatik olarak başlat*, ve *OTR sohbetlerini arşivleme* seçeneklerini Şekil 3'teki gibi **işaretleyin**.

**2. Adım.**  i tıklayarak güvenli anahtarınızı oluşturmaya başlayın; size özel anahtarın oluşturulduğunu belirten aşağıdakine benzer bir mesaj belirecek:



Şekil 4: Özel anahtar oluşturuluyor onaylama kutusu

**Not:** Arkadaşınız da kendi hesabı için aynı adımları takip etmeli

**3. Adım.** Aşağıdakine benzer bir özel anahtar oluşturulduğunda  i **tıklayın**.

Fingerprint: 98737B05 B39BFC18 4597CE0C E513B0DF 59276E3B

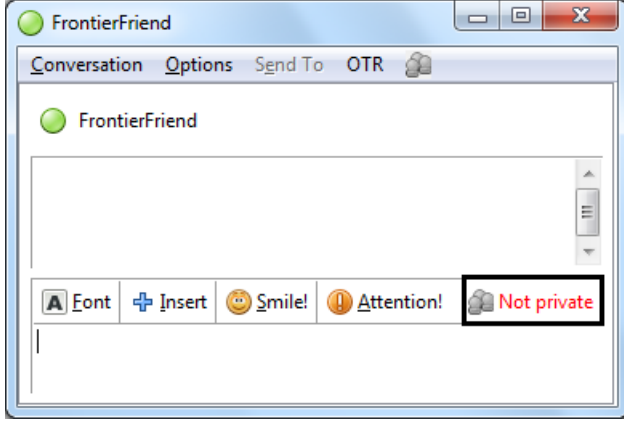
\*Şekil 5: OTR motoru tarafından oluşturulan bir anahtarın örnek bir parmak izi \*

**Önemli:** Şimdi hesabınız için bilgisayarınızda bir özel anahtar yarattınız. Bu konuşmalarınızı şifrelemek için kullanılacak. Böylece sohbet oturumlarınız gözlemlense bile kimse mesajlarınızı okuyamayacak. Parmak izi *Şekil 5'te* gösterildiği gibi belirli bir hesap için bir anahtarı tanımlamaya yarayan uzun bir harf ve rakamlar serisidir.

**Pidgin** sizin ve arkadaşlarınızın parmak izlerini otomatik olarak kaydeder, böylelikle sizin bunları hatırlamanıza gerek kalmaz. **Pidgin'i** yeniden kurar ya da başka bir bilgisayara geçerseniz, ya anahtarınızı yeniden oluşturmak ve arkadaşlarınızın kimliğini yeniden doğrulamalısınız, ya da anahtarınızı ve de arkadaşlarınızın parmak izlerini yeni bilgisayara aktarmalısınız. Bunu yapmak için %APPDATA%.purple (Linux ya da Mac'de ~/.purple) klasörünün içeriğini yeni bilgisayardaki benzer klasöre kopyalamanız gerekir.

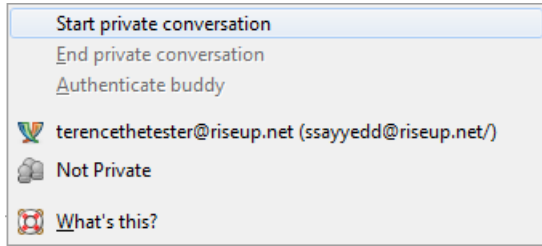
### 3.3 İkinci Adım – Bir Mesajlaşma Oturumu Nasıl Onaylanır?

**1. Adım.** Şu an çevrimiçi olan bir arkadaşın hesabı üstüne **çift tıklayarak** yeni bir **anlık mesajlaşma** oturumu açın. İkiniz de **OTR** eklentisini uygun bir şekilde kurmuş ve yapılandırmışsanız, sohbet pencerenizin sağ alt köşesinde yeni bir **OTR** düğmesinin belirdiğini fark edeceksiniz.



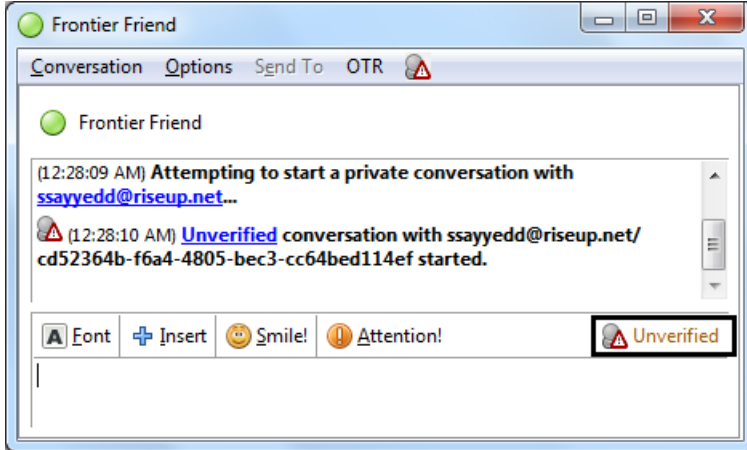
Şekil 6: Siyahla çerçevelenmiş OTR ikonu görülen bir Pidgin mesajlaşma penceresi

**2. Adım.** **Not private**'i tıklayarak açılan menüyü etkinleştirin ve sonrasında **Gizli oturum başlat** öğesini aşağıdaki gibi **seçin**:



Şekil 7:Gizli oturum başlat öğesi seçilmiş olan menü

Pidgin anlık mesajlaşma pencereniz bundan sonra şuna benzeyecek:



Şekil 8: Unverified düğmesini gösteren Pidgin anlık mesajlaşma penceresi

**Not: Pidgin** arkadaşınızın **anlık mesajlaşma** programıyla iletişime otomatik olarak başlar ve özel ve güvenli sohbet oturumlarını başlatmaya yeltendiğinizde mesajları otomatik olarak gönderir. Bunun sonucunda **Not private** OTR düğmesi **Unverified** 'a döner, bu da şu anda arkadaşınızla şifreli bir görüşmede olduğunuzu gösterir.

**Uyarı!** Bu görüşme şimdi güvenli olsa da arkadaşınızın kimliği henüz *teyit edilmedi*. Dikkat edin: arkadaşınız sandığınız kişi aslında arkadaşınızmış *gibi davranan* başka biri olabilir.

### 3.4 Üçüncü Adım – İrtibatta Olduğunuz Kişinin Kimliği Nasıl Teyit Edilir?

**Pidgin** arkadaşınızın kimliğinden emin olabilmek için üç metoddan birini kullanabilirsiniz, 1) önceden belirlediğiniz gizli bir kod kullanabilirsiniz, 2) cevabını sadece ikinizin bildiği bir soru sorabilirsiniz, 3) farklı bir iletişim yoluyla anahtarlarınızın parmak izlerini elle kontrol edebilirsiniz.

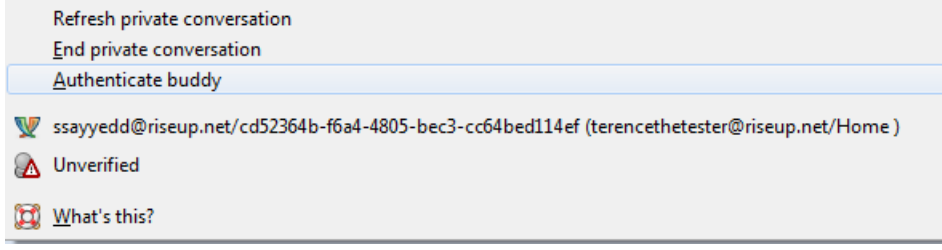
#### Gizli Kod Metodu

Önceden ya yüzyüze bir konuşmada ya da başka bir iletişim vasıtasıyla (telefon, **Jitsi** <sup>[103]</sup> 'de sesli sohbet, ya da cep

telefonu mesajları gibi) bir kod kelime ya da cümleye karar verebilirsiniz. İkiniz de aynı kodu girdiğinizde oturumunuz özgünlüğü teyit edilir.

**Not: OTR** gizli kod tanıma özelliği büyük (A,B,C) ve küçük (a,b,c,) harflere duyarlıdır. Gizli kodunuzu belirlerken bunu aklınızda tutun!

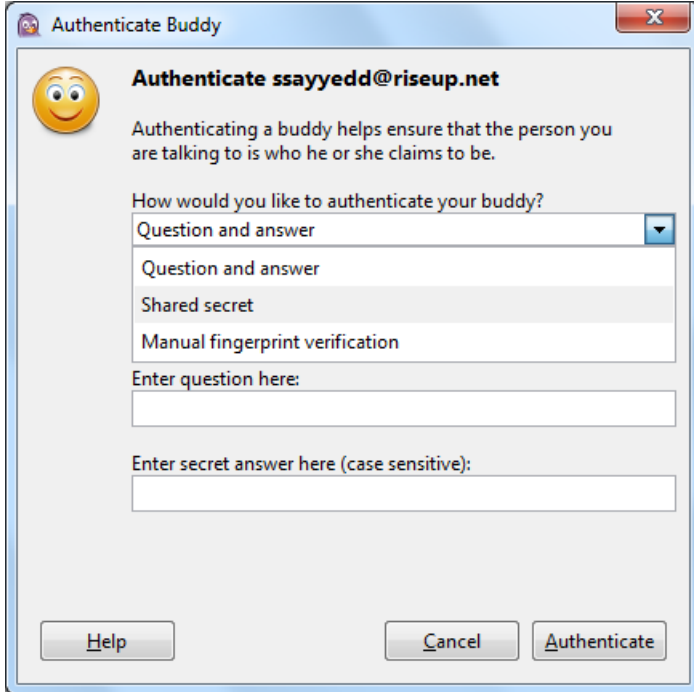
**1. Adım.** Sohbet penceresindeki *OTR* düğmesini **tıklayın**, ve aşağıda görüldüğü gibi *Arkadaşının kimliğini doğrula'yı* seçin:



Şekil 9: Arkadaşının kimliğini doğrula öğesi seçilmiş Teyit edilmemiş menüsü

Bu sizi doğrulama metodunu girmeye davet eden *Arkadaşının kimliğini doğrula* penceresini etkinleştirecek.

**2. Adım.** 'ı tıklayın ve aşağıdaki gibi *Paylaşılan Sır'ı* seçin:



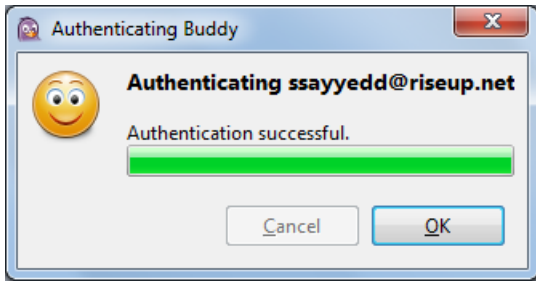
Şekil 10: Aşağı açılır listesi gösterilen Arkadaşının kimliğini doğrula penceresi

**3. Adım.** Gizli kodu aşağıdaki gibi **girin**:



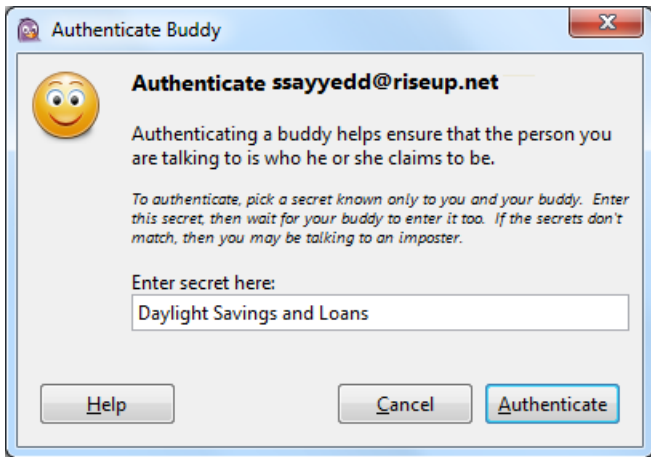
Şekil 11: Paylaşılan Sır penceresi

4. Adım. **Authenticate** i tıklayarak aşağıdaki ekranı etkinleştirin:



Şekil 12: Kurmaca bir irbitat için Arkadaşının Kimliğini Doğrula penceresi

**Not:** Bu anda arkadaşınız Şekil 13'te görülen pencereyi görecektir ve aynı kodu girmesi gerekecek. Eğer kodlar birbirine uyarsa, oturumunuz teyit edilmiş olacaktır.



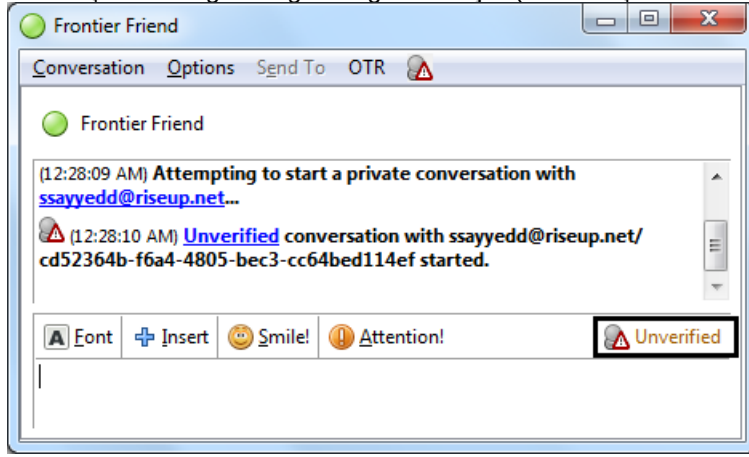
Şekil 13: Kurmaca bir irbitat için Arkadaşının Kimliğini Doğrula penceresi

Oturum teyit edildiğinde **OTR** düğmesi  e dönecek. Bu haliyle oturumunuz güvenli ve gerçekten arkadaşınızla konuştuğunuzdan emin olabilirsiniz.

## Soru Cevap Metodu

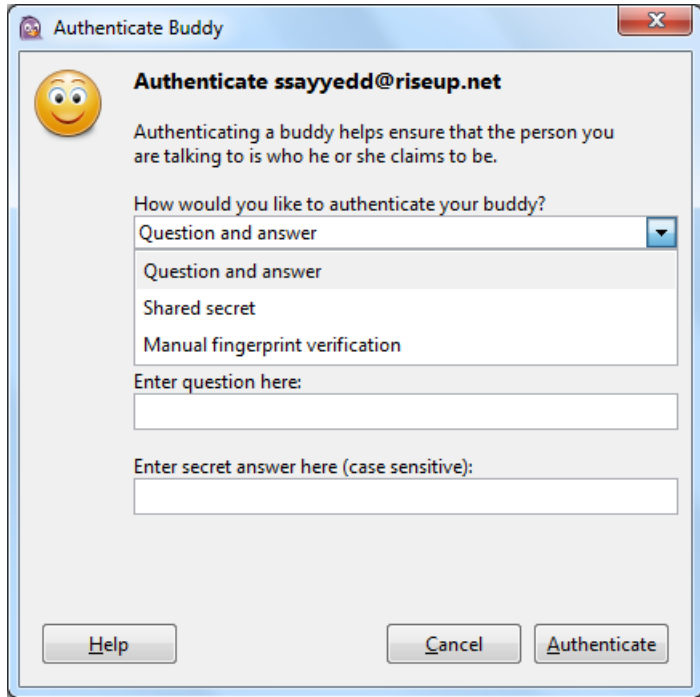
Birbirinizin kimliğini doğrulamanın bir başka yolu da soru cevap metodudur. Bir Soru ve cevabını yaratın. Soruyu okuduktan sonra arkadaşınız *tamamen* aynı cevabı verebilmeli, ve cevaplar birbirini tutarsa, kimlikleriniz otomatik olarak doğrulanacak.

**1. Adım.** Etkin olan bir ileti penceresinde *OTR* menüsünü **tıklayarak** ilgili açılan menüyü etkinleştirin, ve sonrasında *Arkadaşının Kimliğini Doğrula* öğesini **seçin** (lütfen 9. Şekil'e bakın).



Şekil 14: OTR ikonu görünen bir Pidgin sohbet penceresi

**2. Adım.** Aşağı açılır menüyü **tıklayın** ve *Soru Cevap* öğesini aşağıdaki gibi **seçin**:



Şekil 15: Arkadaşının kimliğini doğrula ekranı

**3. Adım:** Bir soru ve cevabını **girin**. Bu soru arkadaşınıza gönderilecek.



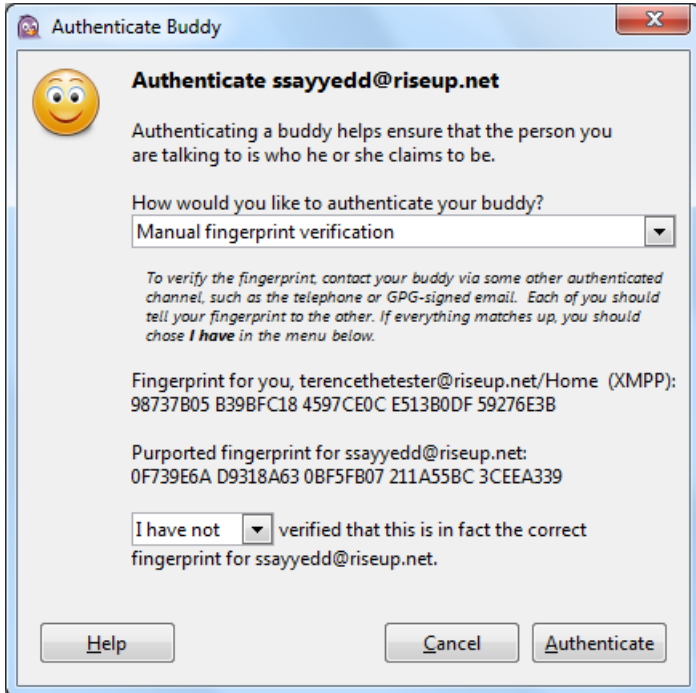
Şekil 16: Soru Cevap ekranı

Arkadaşınızın cevabı sizinkiyle aynıysa, ikinizin de kimliği doğrulanmış, ya da her iki katılımcı da olduğunu iddia ettiği kişi demektir!

Oturumunuzun özgünlüğü teyit edildiğinde *OTR* düğmesi 'a dönecek. Böylelikle oturumunuz güvenli olacak ve arkadaşınızın kimliğinden emin olabileceksiniz..

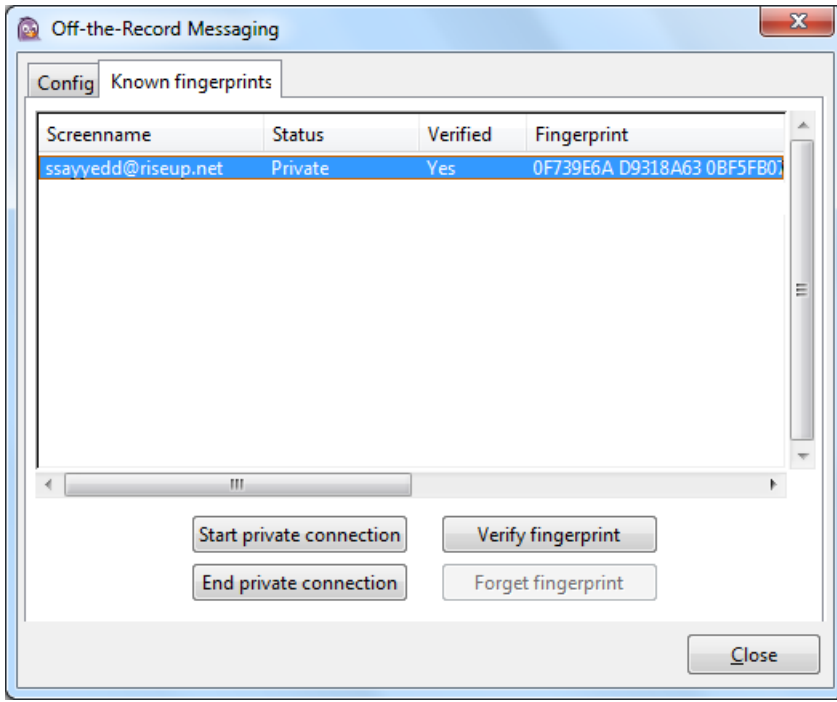
## Elle parmak izi kontrolü

Birbirinizin kimliğini doğrulamanın üçüncü yolu parmak izi kontrolüdür. Bu metodla görünür parmak izlerinizi başka bir iletişim kanalından (güvenli e-posta ya da sesli görüşme gibi) teğış tokuş etmeniz gerekir (aşağıdaki Şekil 17'ye bakınız). Değış tokuş edilen parmak izleri aynı ise, *Bunun gerçekten de doğru parkmak izi olduğunu **doğruladım**'ı* tıklayarak oturumun özgünlüğünü **teyit edebilirsiniz**.



Şekil 17: Elle parmak izi kontrolü ekranı

**Arkadaş listesi > Araçlar > Eklentiler > Off the Record Messaging > Eklenti > Eklentiği Yapılandır**'ı seçtiğinizde, *Tanınan parmak izleri* sekmesi arkadaşınızın hesabını ve kimliğinin doğrulandığını gösterir.



Şekil 18: Tanına Parmak İzleri sekmesi görünen Off-the-Record Mesajlaşma ekranı

Tebrikler! Şimdi gizli bir şekilde sohbet edebilirsiniz. Arkadaşınızla bir sonraki sohbetinizde (aynı bilgisayarları kullanarak), sadece güvenli bir bağlantı talep etmeniz ve arkadaşınızın kabul etmesi yeterli olacak (yukarıdaki Şekil 7 gibi). Oturumunuz böylelikle teyit edilmiş olacak.

## Taşınabilir Pidgin ve OTR

### Short Description:



**Taşınabilir Pidgin** tek bir arayüzle farklı **Anlık Mesajlaşma** hesaplarınızı düzenleyip yönetmenizi sağlayan ücretsiz ve açık kaynak bir istemcidir. **Pidgin**'le kullanım için tasarlanmış **Taşınabilir Off-the-Record (OTR)** eklentisi **Pidgin** kullanıcıları arasında kimliği doğrulanmış ve güvenli iletişimi garanti eder.

### 4.1 Pidgin'in Kurulumlu ve Taşınabilir Versiyonları arasındaki Farklar

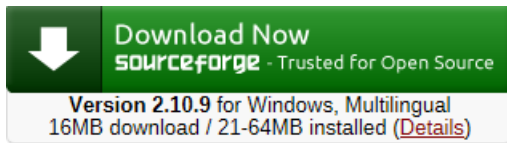
Taşınabilir araçlar bir bilgisayara **kurulmadığı** için, varlıkları ve kullanımları saptanamaz. Fakat, harici aracınız ya da USB bellek çubuğunuz ancak kullandığınız bilgisayar kadar güvenlidir, ve reklam destekli, kötü niyetli ve casus yazılımlar ya da virüs saldırılarına maruz kalabilir.

Bunun dışında Taşınabilir Pidgin ile bilgisayara kurulmak için tasarlanan versiyon arasında hiçbir fark yoktur.

### 4.2 Taşınabilir Pidgin Nasıl İndirilip ve Çıkartılır?

Taşınabilir Pidgin'i indirip çıkartmaya başlamak için aşağıdaki adımları uygulayın:

1. Adım. [http://portableapps.com/apps/internet/pidgin\\_portable](http://portableapps.com/apps/internet/pidgin_portable) [123]'ü **tıklayarak** uygun indirme sitesine yönlendirilin.



2. Adım. **tıklayarak** ilgili **Source Forge** indirme sayfasını etkinleştirin.

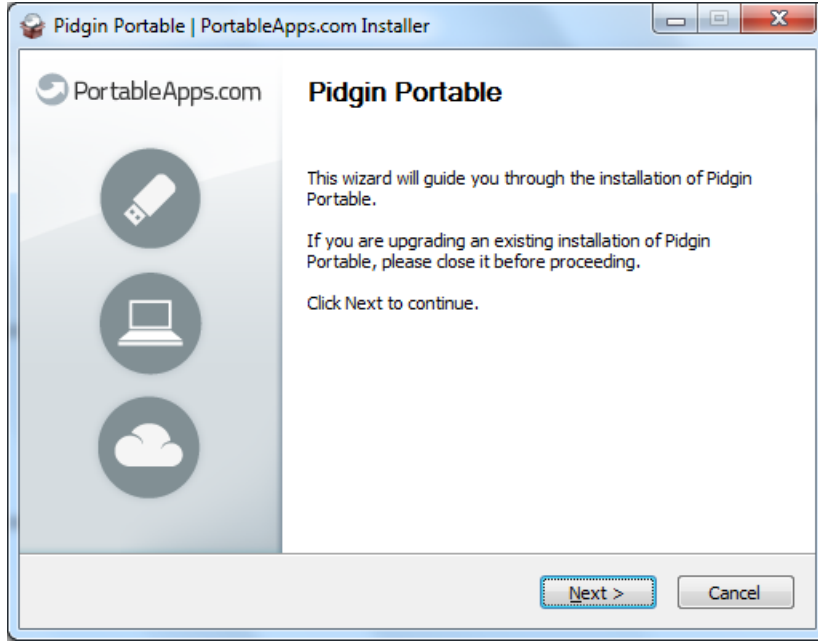
3. Adım. **Kaydet** **tıklayarak** **PidginPortable\_2.10.9.paf.exe** kurulum dosyasını bilgisayarınıza kaydedin, ve indirildiği klasörü **bulun**.

4. Adım. PidginPortable\_2.10.9.paf.exe'ye çift tıklayın, Dosyayı Aç – Güvenlik Uyarısı kutusu belirirse Çalıştır'ı tıklayarak aşağıdaki ekranı etkinleştirin:



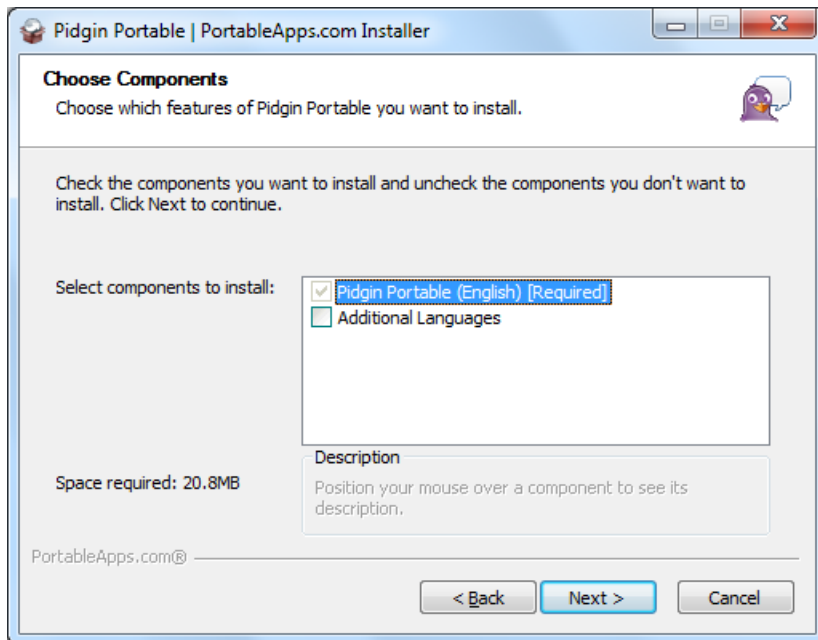
Şekil 1: Kurulum Dili penceresi

5. Adım. OK'ı tıklayarak aşağıdaki ekranı etkinleştirin:



Şekil 2: Taşınabilir Pidgin | PortableApps.com penceresi

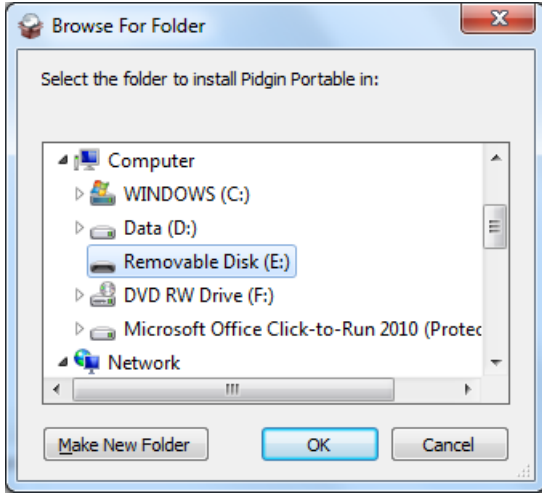
6. Adım. Next >'i tıklayarak aşağıdaki ekranı etkinleştirin:



Şekil 3: Bileşenleri Seç penceresi

**Not: Taşınabilir Pidgin'i** İngilizce'den farklı bir dilde kullanmak istiyorsanız, Diğer Diller seçeneğini işaretleyerek ☐ Additional Languages'i seçin. Bu seçeneğin işaretlenmesi çıkarma işleminin birazcık uzamasına sebep olacak.

7. Adım. **Next >** 'i tıklayarak **Kurulum Yerini Seç** penceresini etkinleştirin, ve **Browse...** 'i tıklayarak aşağıdaki ekranı etkinleştirin:

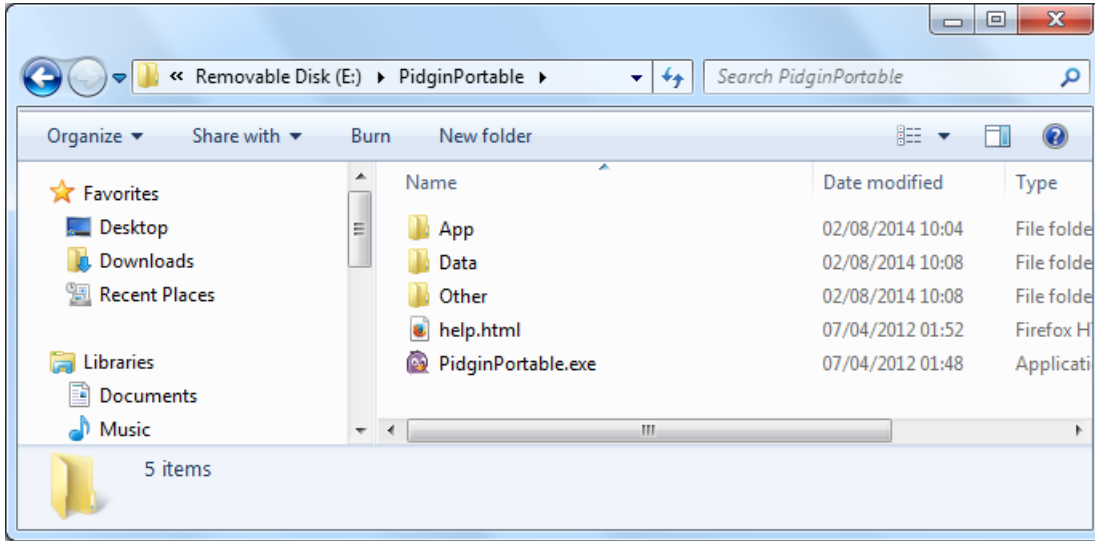


Şekil 4: Klasöre Göz At penceresi

8. Adım. Harici disk ya da USB bellek çubuğuna doğru ilerleyin ve onu seçerek **OK** 'i tıklayıp onaylayın, ve **Kurulum Yerini Seç** penceresine geri dönün.

9. Adım. **Install** 'i tıklayarak belirlediğiniz yere **Taşınabilir Pidgin**'i çıkartma işlemini başlatın, sonrasında **Finish** 'i tıklayarak kurulum işlemini tamamlayın.

10. Adım. Harici diskiniz ya da USB bellek çubuğunuzu aşağıda Şekil 5'te gösterildiği gibi bulup açarak **Taşınabilir Pidgin** programının başarıyla çıkartıldığını teyit edin.



Şekil 5: Klasöre Göz At penceresi

**Taşınabilir Pidgin**'i güvenli ve korunmalı bir şekile kullanmaya başlamadan önce, **Off-the-Record (OTR)** eklentisini indirip çıkartmanız gerekir.

### 4.3 Taşınabilir Pidgin OTR Nasıl İndirilip Çıkartılır?

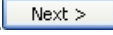
1. Adım. <http://sourceforge.net/projects/portableapps/files/Pidgin-OTR%20Portable/Pidgin-OTR%20Portable%203.2%20Rev%202/> [124] tıklayarak uygun indirme sitesine yönlendirilin.

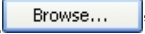
2. Adım. [Pidgin-OTR\\_Portable\\_3.2\\_Rev\\_2.paf.exe](#) 'i tıklayarak **Pidgin-OTR\_Portable\_3.2\_Rev\_2.paf.exe** indirme penceresini etkinleştirin, ve sonrasında **Kaydet** 'i tıklayıp kurulum dosyasını bilgisayarınıza kaydedin.

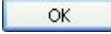
3. Adım. **Çalıştır** 'e çift tıklayın. **Dosyayı Aç – Güvenlik Uyarısı** kutusu açılırsa **Çalıştır** 'i tıklayarak **Kurulum Dili** penceresini etkinleştirin (lütfen Şekil 1'e bakın).

4. Adım. **OK** 'i tıklayarak **Pidgin-OTR Portable | PortableApps.com** penceresini etkinleştirin (lütfen buna benzeyen

Şekil 2'ye bakın).

**5. Adım.** 'ı **tıklayarak Kurulum Yerini Seç** penceresini etkinleştirin (lütfen buna benzeyen Şekil 3'e bakın).

**6. Adım.** 'ı **tıklayarak Klasöre Göz At** penceresini etkinleştirin (lütfen buna benzeyen yukarıdaki Şekil 4'e bakın).

**7. Adım.** Harici diskiniz ya da USB bellek çubuğunuzu **seçip** 'ı **tıklayarak** kurulum yerini onaylayın ve **Kurulum Yerini Seç** penceresine geri dönün.

**8. Adım.** 'ı **tıklayarak Taşınabilir Pidgin**'i belirlediğiniz klasöre çıkarmaya başlayın; 'ı **tıklayarak** kurulum işlemi tamamlayın.

**9. Adım.** Harici diskiniz ya da USB bellek çubuğunuzu Şekil 5'te gösterildiği gibi **bulup Taşınabilir Pidgin** programının klasörünü **açın**.

**10. Adım.**  PidginPortable.exe'ye **çift tıklayarak Taşınabilir Pidgin**'i açın.

**Pidgin**'i yapılandırmaya ve kullanmaya başlamak için lütfen **Pidgin** <sup>[125]</sup> bölümüne bakın.

#### Offline Installation Instructions :

#### Pidgin ve OTR'yi kurma

- *Kısa Uygulamalı-Rehber'in* <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Pidgin** ve **OTR** ikonlarını **tıklayın** ve kurucuları 'Açın' ya da 'Çalıştırın'. Gerekirse önce kurucuyu indirin ve sonra yerini bulup üstüne çift tıklayın
- Devam etmeden önce bir sonraki kısımdaki 'Kurulum Yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulumdan sonra silebilirsiniz

**Pidgin: OTR:**



[126]

Off-the-Record

[127]

## Sıkça Sorulan Sorular ve Gözden Geçirme

### 5.0 Sıkça Sorulan Sorular ve Gözden Geçirme

**Soru: Pidgin-OTR'yi arkadaşlarımla MSN ve Yahoo'da sohbet için kullanabilir miyim??**

**Cevap:** **Pidgin-OTR** farklı sohbet ve mesajlaşma servislerini desteklese de çoğu zaman arkadaşınızla **anlık mesajlaşma** oturumu açabilmeniz için ikinizin de aynı sağlayıcıyı kullanmanız gerekir. Örneğin, ikinizin de **IRC** ya da **ICQ** hesabını kullanması gerekir. Fakat, **XMPP** protokolünü kullanan servisler (**RiseUP**, **Google Talk**, **Facebook**, ya da diğer **XMPP** sunucuları gibi) birbirlerinin hesapları arasında sohbete izin verebilirler. Böylelikle **RiseUp** ve **Google Talk** hesapları arasında bir sohbet kurulabilir. Bunun yanında unutmayın ki **Pidgin** ile aynı anda birkaç **anlık mesajlaşma** hesabını kaydedip hepsi üzerinden çevrimiçi olabilirsiniz. Bu da çok protokollü anlık mesajlaşma istemcisi kullanmanın iyi yanı.

**Soru: Pidgin-OTR hesabıma başka bir bilgisayardan nasıl ulaşabilirim?**

**Cevap:** Bunu yapmanın bir yolu o bilgisayar üzerinde **anlık mesajlaşma** hesabınızla kullanılmak üzere yeni bir özel anahtar oluşturmaktır, ama oturumunuzun özgünlüğünü yeniden teyit etmeniz gerekecek. Bir başka seçenek de şifreleme anahtarlarınızı yeni bilgisayarınıza kopyalamaktır (bunları Windows'ta %APPDATA%.purple içinde ve Linux ve Mac'te ~/.purple içinde bulabilirsiniz).

**Soru: Ya anlık mesajlaşma hesabımın parolasını unutacak olursam? Ya da başka biri bunu eline geçirirse? Geçmiş ve gelecekteki bütün konuşmalarıma ulaşabilecekler mi?**

**Cevap:** Bu çok önemli bir soru. Öncelikle, parolanızı unutursanız ve hesap sağlayıcınızın önerdiği yollarla yenileyemiyorsanız yeni bir **anlık mesajlaşma** hesabı oluşturmanız gerekecek. Bundan sonra, arkadaşınızı birbirinizi tanıyabileceğiniz güvenli ve teyit edilmiş bir e-posta ya da sesli sohbet yoluyla bilgilendirmelisiniz.

Son olarak birbirinizi arkadaş olarak teyit etmelisiniz. Başka biri her hangi bir yolla **anlık mesajlaşma** parolanızı eline geçirmişse, o kişi **Pidgin** kullanırken sizmiş gibi davranmaya yeltenebilir. Neyse ki, sizin şifreleme anahtarlarınız ya da sizin paylaştığınız parola kelimeleri bilmediği için oturumu teyit edemeyecek. Böylelikle arkadaşınız ondan şüphe edebilir. İşte bu yüzden kimlik doğrulama **çok** önemlidir.

Ek olarak, yukarıdaki yönergeleri takip edip **OTR'nin** 'Yapılandırma' sekmesinde tavsiye edilen seçenekleri ayarladıysanız, parolanızı çalan ya da bilgisayarınıza ulaşımı olan biri bile geçmiş görüşmelerinize ulaşamayacak, çünkü onları kaydetmemeyi seçtiniz.

## 5.1 Gözden Geçirme Soruları

- Bir arkadaşınızla sohbet oturumunuzu kaç defa teyit etmeniz gereklidir?
- Pidgin'de birden fazla anlık ileti hesabını kaydedip aynı anda kullanmak mümkün müdür?
- Pidgin'de parmak izi ne demektir?
- Başka bir bilgisayarda Pidgin-OTR'yi kurduğunuzda OTR seçeneklerinize (alınan anahtarların parmak izleri dahil olmak üzere) ne olacak?
- Pidgin'de özel ve teyit edilmiş bir sohbet oturumu açmak için neler gereklidir?
- Pidgin'de bir hesap açmak için ne gerekir?

## Jitsi – Güvenli Sesli, Görüntülü ve Anlık Mesajlaşma

### Short Description:

**Jitsi**, internet üzerinden **Anlık Mesajlaşma** (Instant Messaging, **IM**), işitsel ve görsel sohbeti destekleyen, farklı sunucularla çalışabilen, **ücretsiz ve açık kaynak kodlu** <sup>[128]</sup> bir platformdur. En popüler ve sıklıkla kullanılan **IM** ve telefonculuk protokollerini destekler. Bunlara **SIP** ( **Session Initiated Protocol**, Oturumla Başlatılan Protokol), **Jabber/XMPP** (**Facebook** ve **Google Talk**), **AIM**, **ICQ**, **MSN** ve **Yahoo! Messenger** dahildir. Yazılı sohbetlere **OTR (Off-the-Record)** <sup>[129]</sup> protokolü üzerinden ek bir bağımsız şifrelemenin yanında, ve işitsel ve görsel (**ZRTP**, **SRTP**) oturumlar sunar. **Jitsi**, **Microsoft Windows**, **Mac OS** ve **Linux** üzerinden çalışır. Ayrıca **Android** versiyonu da geliştirilmektedir.

### Online Installation Instructions:

#### Jitsi'yi İndirmek

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Jitsi** ikonunu **tıklayın** ve **https://jitsi.org/Main/Download** web sitesini açın
- **Jitsi 2.4 and stable build line** bölümünden **Microsoft Windows installers** linkini **tıklayın** ve kurulumcu dosyayı kaydedin. Daha sonra, kaydettiğiniz yere **gidin** ve dosyanın üzerine **çift tıklayın**



[130]

#### Ana Sayfa

- <https://jitsi.org/> <sup>[131]</sup>

#### Bilgisayar Gereksinimleri

- Tüm Windows Sürümleri

#### Bu Rehberde Kullanılan Sürüm

- 2.4

#### Bu bölümün son güncellenme tarihi

- Ocak 2014

#### Lisans

- Ücretsiz ve Açık kaynak yazılım

#### Buradan sağlayacağınız faydalar:

- Video sohbet oturumlarını da içeren gizli ve güvenli entegre iletişim sistemine sahip olmak.
- İletişiminizi hesap sunucularınızdan bağımsız olarak şifreleme imkanı.
- Aynı anda farklı hesapları (örneğin **Facebook**, **Google Talk**, **Yahoo Messenger**) kullanma imkanı.

#### GNU Linux, Mac OS ve Microsoft Windows ile çalışan diğer programlar:

**Jitsi**, **GNU Linux**, **Mac OS** ve **MS Windows** ile çalışır (yakın zamanda **Android OS** ile de). **Jitsi'nin** bağımsız **OTR** veya **ZRTP** şifrelemeleri kullanarak iletişim kurabildiği diğer programlar aşağıdaki gibidir: Yazılı mesaj için: **Pidgin** <sup>[78]</sup> (**MS Windows** ve **GNU Linux**), **Miranda** <sup>[104]</sup> (**MS Windows**), **Adium** <sup>[132]</sup> (**Mac OS X**), **ChatSecure** <sup>[133]</sup> (**Android OS** and **iOS** daha önce **Gibberbot** <sup>[134]</sup> olarak bilinirdi). Video aramaları için: **CSipSimple** (**Android OS**), **Linphone** <sup>[135]</sup> (**GNU Linux**, **MS Windows**, **Mac OS X**, **Android OS**, **iOS**, ve diğerleri.)

## .1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

**Jitsi**, birçok farklı hesap çeşidini ve iletişim protokolünü destekler ve böylelikle farklı programlar kullanan kişilerle iletişim kurmanızı sağlar. Bu programlardan bazıları, benzer şekilde iletişiminizin güvenliğini sağlamak için, bağımsız metin ve ses şifrelemeyi (**OTR** ve **ZRTP**) destekleyen çeşitli özellikler sunar (yukarıda adı geçen programlar gibi). Fakat, özellikle tescilli olan diğer programlar (**Facebook** sohbet veya **Google Talk** gibi) bu özelliklere sahip olmayabilir. Yine de, bu tescilli programları kullanan kişiler ile **Jitsi'nin** yardımı ile iletişim kurabilirsiniz, fakat bu durumda **Jitsi'nin** ek güvenlik özelliklerinden faydalanamazsınız.

**Facebook Sohbet, Google Talk, Yanoo! Messenger, Skype** veya **Viber** gibi servislerin sunucuları metin, ses veya video ile kurduğunuz iletişimlerin oturumlarına erişebilir ve gerektiğini düşündükleri zaman bunları, şirketler ve hükümetler gibi üçüncü taraflar ile paylaşabilir. **Jitsi**, var olan hesaplarınızı kullanırken bunlara ek şifreleme getirerek daha gizli ve güvenli şekilde iletişim kurmanızı sağlar. Bu şekilde, iletişiminizin içeriği hesap sunucularının ve potansiyel üçüncü tarafların erişimine kapalı olur. Özel sohbet oturumlarınız ve iletişimlerinizi korumak için, **Jitsi**, yazılı sohbetler için **Off-the-Record (OTR)** <sup>[129]</sup> ve sesli aramalar için **ZRTP/SRTP** gibi kriptograflık yöntemler kullanır.

**Jitsi** ve **Skype** gibi programların arasındaki en önemli farklardan bir diğeri, **Jitsi'nin** kullanıcılarını program geliştiricilerden bağımsız bir şekilde farklı servis sunucularına bağlı hesaplarını kullanmalarını sağlamasıdır. Bu demektir ki, **Jitsi** kullanmadan önce bir hesap oluşturmanız gerekir.

**Not: Jitsi, Java** programlama dilini kullanır. Bu yüzden, çalışması için Java programının bilgisayarınıza kurulu olması gerekir. **Oracle Java'nın** birçok güvenlik zaafı olduğu bilinmektedir, bunlar aracılığıyla bilgisayarınızın yönetimi uzaktan erişimli kullanıcılar tarafından ele geçirilebilir ve iletişim ve verilerinize erişmek için bilgisayarınıza casus yazılım kurulabilir. Bilgisayarınızda Java kullanabilen programların sayısını mümkün olduğunca azaltmanızı **şiddetle** tavsiye ederiz. Lütfen, **Firefox'ta Java ile ilişkili eklentileri devre dışı bırakmak** <sup>[136]</sup> ve **bilgisayarınızdaki tüm tarayıcılar için Java'yı devre dışı bırakma adımları'na** <sup>[137]</sup> bakın. Fakat, bu bölümde daha sonra göreceğiniz gibi, **Java** gerektirmesine rağmen, **Jitsi** kullanmanın çeşitli güvenlik faydaları vardır.

### Offline Installation Instructions :

#### Installing Jitsi

- Kısa **Uygulamalı Rehberler'in** <sup>[138]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Jitsi** ikonunu **tıklayın** ve kurulumcuyu 'Aç'ın, ya da 'Çalıştır'ın. Gerekirse, kurulumcuyu öce kaydedin, sonra kaydettiğiniz yere gidip üzerine çift tıklayın
- Devam etmeden önce bir sonraki bölümdeki Kurulum Bilgileri'ni okuyun
- \*Kurulumcuyu bilgisayarınıza kaydettiyseniz, kurulumdan sonra silebilirsiniz. \*

**Jitsi:**

□ <sup>[139]</sup>

## Jitsi- Jitsi Nasıl Kurulur ve Jitsi'ye Farklı Hesaplar Nasıl Eklenir?

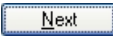
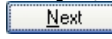
Bu sayfadaki bölümlerin listesi:

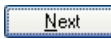
- **2.1 Jitsi nasıl kurulur?**
- **2.2 Jitsi'ye farklı hesaplar nasıl eklenir?**
- **2.2.1 Gmail-Google hesabı nasıl eklenir?**
- **2.2.2 Yeni Jabber/XMPP veya SIP hesabına kaydolmak ve bunu Jitsi'ye eklemek**
- **2.2.3 Facebook hesabı nasıl eklenir?**
- **2.3 Jitsi ile hesap parolası değiştirilir?**
- **2.4 Güvenliğini arttırmak için Jitsi nasıl yapılandırılır?**
- **2.4.1 Arama ve sohbet geçmişini devre dışı bırakma ve silme**
- **2.4.2 Yazılı sohbette özel mesaj isteği**
- **2.4.3 Ana parola ile hesaplarınızın parolalarını koruma**

### 2.1 Jitsi nasıl kurulur?

Jitsi'yi kurmak için aşağıdaki adımları takip ediniz:

**1. Adım.**  **jitsi-2.4-latest-x86.exe** 'ye çift tıklayın, 'Dosyayı Aç – Güvenlik Uyarısı' kutusu görünürse **Winows Kurulum** ekranını etkinleştirmek için **Çalıştır**'ı **tıklayın**. Bu sizi, **Jitsi Kurulum Sihirbazına Hoşgeldiniz** penceresine götürecektir.

**2. Adım.** **Son Kullanıcı Lisans Anlaşması** penceresini etkinleştirmek için 'i **tıklayın**, **Lisans Anlaşması**ndaki maddeleri kabul ediyorum'u tıklayın ve **Hedef Klasör** penceresini etkinleştirmek için 'i **tıklayın**.

**3. Adım.** **Ek Görevler** penceresini etkinleştirmek için 'i **tıklayın** ve verili ayarları olduğu gibi **kabul edin**.

**Not:** **Bilgisayar açıldığında ya da yeniden başladığında otomatik olarak başla** seçeneğini seçmek bilgisayarınızın genel

hızını düşürebilir, özellikle de bilgisayarınız açıldığında başlaması için programlanmış birden fazla uygulamanız varsa.

**4. Adım.** *Jitsi'yi Kurmaya Hazır* penceresini etkinleştirmek için **Next** i tıklayın ve kurulum ilerleme çubuğunu gösteren *Jitsi'yi Kuruluyor* penceresini etkinleştirmek için **Install** i tıklayın.

**5. Adım.** Kurulum işlemini tamamlamak ve aşağıda görüldüğü gibi **Jitsi Giriş yap** penceresini otomatik olarak açmak için **Finish** i tıklayın:

Sign in

Configure all your favorite protocols in one click.

**SIP SIP**

Username

Ex: john@voipphone.net or simply "john" for no server

Password

**XMPP**

Username

Ex: johnsmith@jabber.org

Password

**Facebook**

Username

Ex: username

Password

**Google Talk**

Username

Ex: johnsmith@gmail.com or johnsmith

Password

[NOT REGISTERED YET?](#)

**MSN**

Username

Ex: johnsmith@hotmail.com

Password

[NOT REGISTERED YET?](#)

**AIM**

Username

Ex: johnsmith

Password

[NOT REGISTERED YET?](#)

**ICQ**

Username

Ex: 83378997

Password

[NOT REGISTERED YET?](#)

**Yahoo!**

Username

Ex: johnsmith@yahoo.com or johnsmith

Password

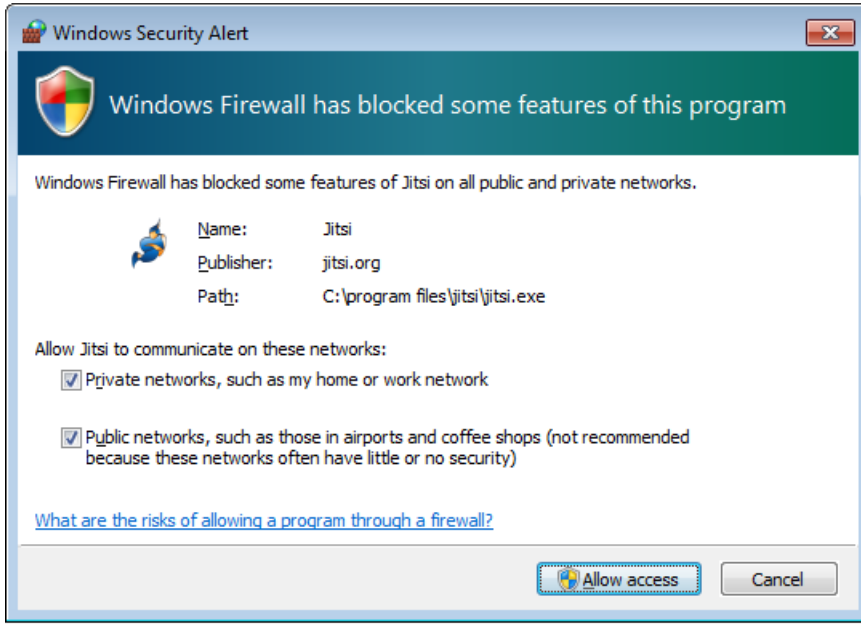
[NOT REGISTERED YET?](#)

[Use online provisioning](#)

Sign in Cancel

Şekil 1: Jitsi Giriş yap penceresi

**Not:** Jitsi'nin ilk defa kurulduğu ve başlatıldığı bazı durumlarda, *Windows Güvenlik Uyarısı* ekranı belirebilir (aşağıda Şekil 2). **MS Windows** işletim sistemi için bu uyarı normaldir. **Jitsi'yi** kullanmaya devam etmek bir sorun yaratmaz. Düğmelerden herhangi birine basarsanız ve uyarı penceresini kapatsanız bile, **Jitsi**, **Jabber/XMPP** veya **SIP**, **Google Sohbet**, **Facebook Sohbet**, veya **Yahoo Messenger** gibi olağan kamusal servisleri kullanarak iletişim kurmaya yetkindir. Fakat, **Ulaşım izin ver** düğmesini tıklamak, **Registrarless SIP Hesapları** isimli, gelişmiş bir **Jitsi** özelliğinin çalışmasını sağlar. Bu özel hesaplarla ilgili daha fazla bilgi için, lütfen **Registrarless SIP Accounts** <sup>[140]</sup> sayfasına bakın.



Şekil 2: Windows Güvenlik Uyarısı ekranı

**6. Adım. Açık ve Özel ağlar kutularının her ikisini de işaretleyin ve Jitsi Giriş yap penceresini (yukarıdaki Şekil 1'de görüldüğü gibi) veya ana kullanıcı arayüz penceresini (aşağıdaki Şekil 4'te görüldüğü gibi) görmek için Erişime İzin Ver'i tıklayın.**

## Jitsi'ye farklı hesaplar nasıl eklenir?

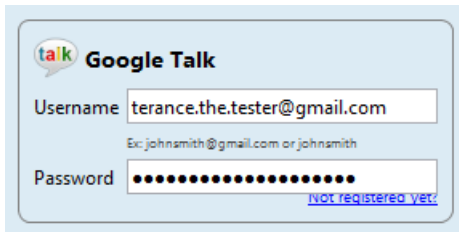
Bu kısım, farklı tipteki hesapların nasıl **Jitsi'ye** ekleneceği ile ilgilidir. **Jitsi**, birçok farklı hesap tipini destekler. Aşağıda belirttiğimiz hesaplar genellikle **Jabber/XMPP** ve **SIP** iletişim protokollerine dayalıdır. Birçok servisin yanı sıra, **Jitsi**, **Gmail** veya **Facebook** hesaplarınızı da kullanmanıza izin verir. Bunlar Internet'te kullanılan en popüler servisler olduğu için, onları **Jitsi'ye** nasıl ekleyebileceğiniz aşağıda gösterilmiştir. Aynı zamanda, bu hesapları kullanırken, hesap sunucularınız tarafından sunulanın üstüne **Jitsi'nin** bağımsız şifrelemesini kullanarak güvenliğinizi nasıl arttıracacağınız konusunda da bilgi verilmiştir. Fakat aklınızda bulundurun ki, **Jitsi** şifrelemesi ile bile, **Google** veya **Facebook** gibi hesap sunucuları iletişim halinde olduğunuzu (ve büyük ihtimalle kimlerle iletişim kurduğunuzu) takip eder ve şirketler ve hükümetler gibi üçüncü taraflarla bilgilerinizi paylaşabilir. Bu yüzden, hassas bilgilerin dahil olduğu iletişim için, **Jitsi** şifrelemesi olsa bile, bu hesapları kullanmamak daha iyi olabilir. Bu bölümde aynı zamanda, nasıl daha güvenli hesaplar (Jabber/XMPP veya SIP) yaratabileceğinizi ve bunları **Jitsi'ye** nasıl ekleyeceğinizi de anlatıyoruz ve bu hesapları kullanmanızı tavsiye ediyoruz.

### Gmail-Google hesabı nasıl eklenir?

**Not:** Aşağıdaki örnek bir **Google Talk** hesabından alınmıştır. Yukarıdaki Şekil 1'de listelenen diğer iletişim protokollerinin kurulumu benzerdir. İletişim veya bazı özellikler (**Jitsi** bağımsız şifreleme veya yazılı sohbet ve ses – **OTR** ve **ZRTP**), farklı hesap sunucuları (Facebook, Gmail, Yahoo ve benzeri) arasında çalışmayabilir. Fakat, aynı servis sunucusuna sahip hesaplar arasındaki iletişimde çalışmalıdır.

**1. Adım. Başla > Jitsi'yi seçin** – veya **Jitsi** masaüstü ikonuna **çift tıklayarak Jitsi'yi** açın.

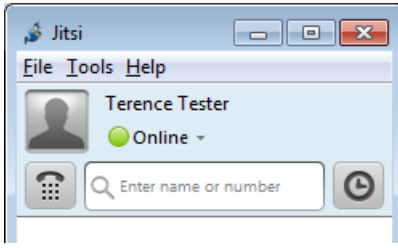
**2. Adım. Giriş yapın** penceresine, **Gmail** hesabınıza ait, sohbet amaçlı kullanmak istediğiniz kullanıcı adı ve parolasını **yazın**. Aşağıdaki gibi görünecektir:



Jitsi 'Giriş Yap' penceresi (boyutu değiştirilmiş)

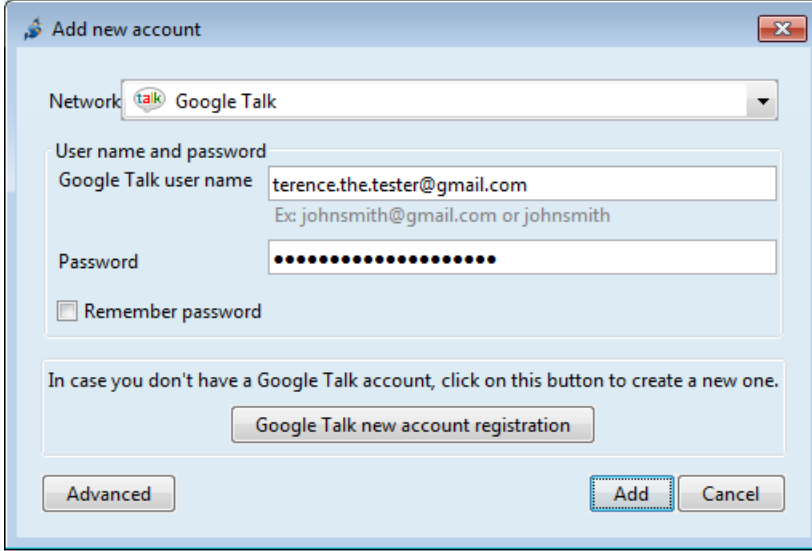
**Not:** Aynı anda farklı protokoller kullanarak birden fazla hesap ekleyebilirsiniz.

**3. Adım.** Hesabınızın sohbet penceresini aşağıda görüldüğü gibi etkinleştirmek için **Sign in** butonuna **tıklayın**:



Şekil 4: Gmail hesabını ekledikten sonra Jitsi ana penceresi örneği

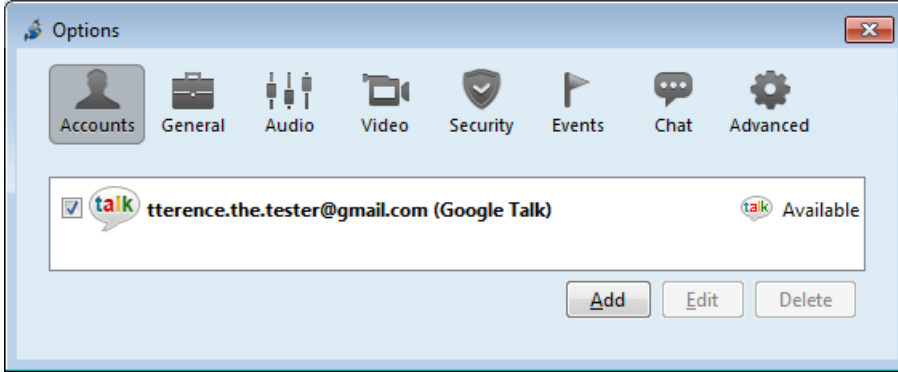
**Not:** Giriş yap penceresini kapattıysanız ya da başka bir hesap eklemek istiyorsanız, bunu **Klasör > Yeni hesap ekle...** menüsünü **seçerek** ekleyebilirsiniz. Yeni pencerede, **Ağ'ı Google Talk** olarak **seçin** ve **Gmail** hesabınızın kullanıcı adı ve parolasını aşağıda görüldüğü gibi yazın:



Şekil 5: 'Yeni hesap ekle' penceresi

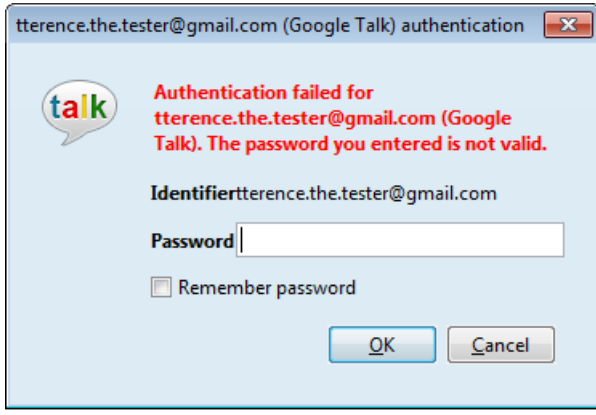
**Gmail** hesabınızı **Jitsi**'ye kaydettiğinizden emin olmak için aşağıdaki adımları takip edin:

**1. Adım.** Aşağıdaki pencereyi etkinleştirmek için menüden **Araçlar > Seçenekler'i** seçin:



Şekil 6: Yeni kayıtlı Gmail hesabını gösteren Seçenekler menüsü (boyutu değiştirilmiş)

**Not:** Gmail hesabınıza erişimi korumak için **2 adımlı doğrulama** <sup>[141]</sup> kullanıyorsanız, her zamanki parolanız ile **Jitsi**'den giriş yapmayı denediğiniz zaman aşağıdaki gibi bir mesaj ile karşılaşabilirsiniz. **Jitsi** kullanarak giriş yapmak için, 'uygulamaya özel parola' üretmeniz gerekir. Bunu nasıl yapabileceğinizi öğrenmek için Google'un yönergelerini takip ederek <sup>[142]</sup> öğrenin..



Şekil 7: Google Talk giriş kimlik doğrulama başarısız örneği

## 2.2.2 Yeni Jabber/XMPP veya SIP hesabına kaydolmak ve bunu Jitsi'ye eklemek

**Jabber/XMPP** ve **SIP**, yazılı ve sesli iletişim açık standartlarıdır. Jitsi ile birlikte kullanabileceğiniz, bedava hesap sunan birçok sunucu [143] vardır. Aşağıda, hassas bilgi içeren iletişimde kullanabileceğiniz bazı sunucular tavsiye ediyoruz. Aklınızda tutun ki, **Jabber/XMPP sunucu yazılımı** [144] (**ejabberd** [145] veya **Prosody IM** [146] gibi) indirmek de mümkündür. Bunları kendi sunucu bilgisayarınıza indirebilir, grup, topluluk ve organizasyon üyelerini arasında güzlü ve güvenli iletişim kurmak için kullanabilirsiniz.

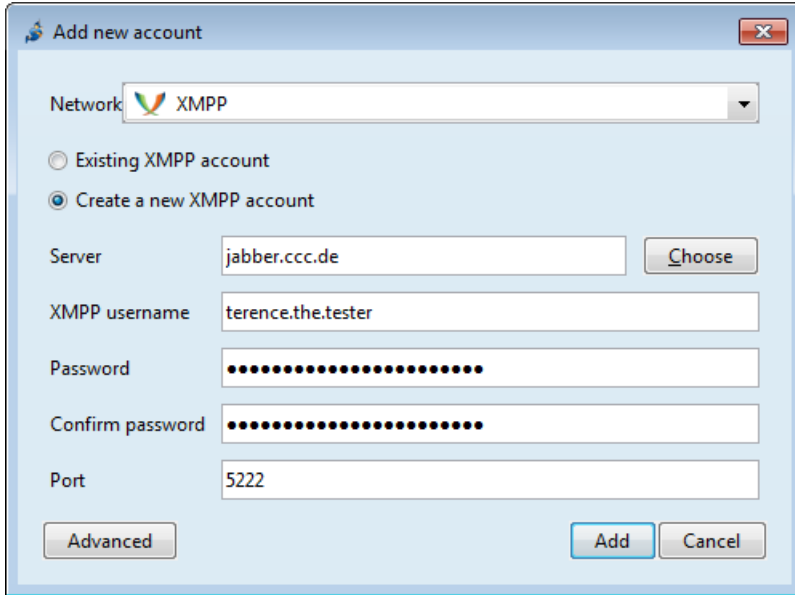
- **Riseup.net** Jabber/XMPP hesabı

**Riseup.net güvenli e-posta servisi** [119] (Amerika bazlıdır) üzerinde hesabınız varsa, bu hesabı Jitsi'ye ekleyerek, **Jabber/XMPP ağı üzerinden iletişim kurmak** [147] için kullanabilirsiniz. Var olan Jabber/XMPP hesabını nasıl ekleyeceğinizi öğrenmek için aşağıya bakın.

- **Jabber.ccc.de** ve diğer Jabber/XMPP hesapları

Bir hesabı Jabber.ccc.de sunucusu üzerine (Almanya bazlıdır) kaydetmek için aşağıdaki adımları takip ediniz:

**1. Adım. Jitsi'de** menüden **Dosya > Yeni hesap ekle...**'yi seçin. Yeni açılan pencerede, **Ağ: XMPP'yi seçin** ve **Yeni XMPP hesabı aç** seçeneğini **işaretleyin**. Sunucuya jabber.ccc.de **yazın**, yaratmak istediğiniz XMPP kullanıcı adını **yazın** ve **Parola**, ardından da **Parolayı Onayla** alanlarını **doldurun**. Ekran aşağıdaki gibi görünecektir:



Şekil 8: 'Yeni XMPP hesabı yarat' seçili 'Yeni hesap aç' penceresi örneği

**2. Adım. Ekle'yi tıklayın.** Başarılı bir kayıt işleminden sonra yukarıdaki Şekil 4'e benzeyen bir pencere göreceksiniz.

Kullanıcı adınız başkası tarafından alınmışsa, kayıt işlemi, *Bir hata yüzünden kayıt işleminiz tamamlanamadı: Veriler onaylanamıyor.* mesajı vererek başarısız olacaktır. Farklı bir kullanıcı adı seçerek işlemi yeniden tekrar edebilirsiniz.

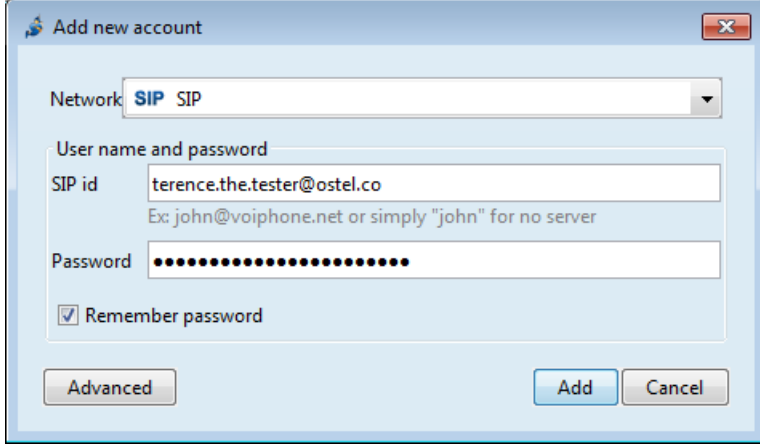
Jabber.ccc.de hesabınıza 12 aydan uzun bir süre giriş yapmazsanız, hesabınız otomatik olarak sunucudan kaldırılacak ve kullanıcı adınız başkalarının kullanımına açılacaktır.

Bahsedilmeye değer bir başka Jabber/XMPP sunucusu ise **jitsi.si**'dir. Bu sunucu **Jitsi** programını geliştirenler tarafından korunur. **jitsi** [148] ve diğer Jabber/XMPP sunucularında yukarıdaki bölümde anlatıldığı gibi hesap oluşturabilirsiniz. IM

Observatory, [kamusal Jabber/XMPP sunucularının listesini](#) <sup>[143]</sup> tutar ve herhangi bir Jabber/XMPP sunucusunun güvenliğini test etmenizi sağlar <sup>[149]</sup>.

- **ostel.co** SIP hesabı

**SIP** hesaplarına **Jitsi** programının içinden kayıt olunamaz. **Ostel.co** sunucusu (Amerika bazlıdır) kendi [web sayfalarında](#) <sup>[150]</sup> kayıt olma hizmeti sunar. Bir kullanıcı adı ve parola **seçtikten** ve e-posta adresinizi belirttikten sonra web sayfasındaki **Giriş Yap** düğmesine **basın**. Başarılı bir şekilde kayıt yaptıktan sonra Jitsi programına geri **dönün**. Menüden **Dosya > Yeni hesap ekle**'yi **seçin Ağ: SIP'yi seçin** ve kullanıcı adınızı (örneğin, terence.the.tester@ostel.co) ve web kaydı esnasında yarattığınız parolayı **girin**, ardından **Ekle'yi tıklayın**. Örnek olarak aşağıdaki görüntüye bakabilirsiniz:



Şekil 9: SIP hesabı için 'Yeni hesap ekle' penceresi örneği

- **Var olan Jabber/XMPP veya SIP hesaplarını Jitsi'ye eklemek**

Hali hazırda Jabber/XMPP veya SIP hesabınız varsa, onları, menüden **Dosya > Yeni Hesap ekleyin...**'i seçerek ve uygun olan **Ağ**'ı (hesap türüne bağlı olarak XMPP veya SIP) belirleyerek **Jitsi'ye** ekleyebilirsiniz.

### 2.2.3 Facebook hesabı nasıl eklenir?

**Jitsi'nin** Facebook sohbetinize bağlanabilmesi için, **Facebook'taki** iki ayarı değiştirmeniz gerekebilir

- **Facebook Kullanıcı adı**

**Facebook**, **Jitsi'nin** Facebook sohbete bağlanabilmesi için bir kullanıcı adı ister. Birçok **Facebook** kullanıcısının zaten bir kullanıcı adı vardır. Kullanıcı adınıza bakmak için **Facebook** hesabınıza **girin**. Zaman Tüneli veya Sayfanızı görüntülediğinizde konum çubuğunda <https://www.facebook.com/> 'dan sonra görünen kullanıcı adınızdır. Aynı zamanda, Kişisel hesabınızın **Facebook** e-posta adresinde de kullanıcı adınızı görebilirsiniz (örneğin, kullanıcıadı@facebook.com). Kullanıcı adınızı görmek, değiştirmek veya ilk defa almak için **Hesap Ayarları > Genel** bölümüne gidebilir veya <https://www.facebook.com/username> <sup>[151]</sup> sayfasını ziyaret edebilirsiniz. Kullanıcı adı oluştururken, **Facebook** hesap onaylamanızı gerçekleştirirken cep telefonu numaranıza mesaj göndermeyi şart koşabilir. Daha fazla detay için, [Facebook'un kullanıcı adı ile ilgili açıklamalarına](#) <sup>[152]</sup> bakabilirsiniz

- **Uygulama Ayarları**

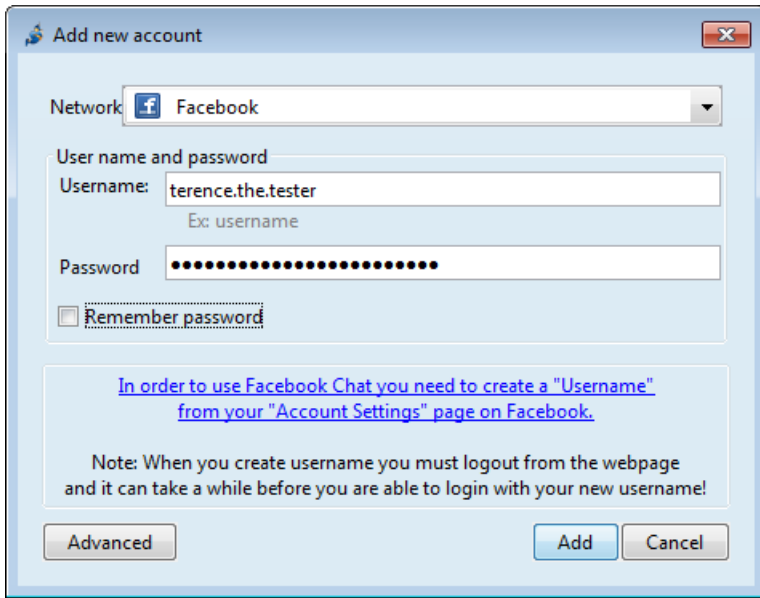
**Jitsi** Facebook Sohbe bağlanmadan önce **Facebook'un** 'uygulama platformu' etkinleştirilmeli. **Facebook Hesap Ayarları > Uygulamalar** bölümüne gidin ve **Kullandığınız uygulamalar** için **Açık** seçeneğinin işaretli olduğundan emin olun. Bunu yapmak, hesabınız için 'uygulama platformunu' açacaktır.

**Aklınızda tutun** ki, **Facebook'un** 'uygulama platformu'nu açmak **Facebook** verilerinizin büyük bir kısmını üçüncü taraf uygulama geliştiricilerine açık hale getirir. Bu şekilde, verileriniz sadece kullandığınız **Facebook** uygulamalarına değil, arkadaşlarınızın kullandığı **Facebook** uygulamalarına da açık hale gelir. **Facebook'un** 'uygulama platformu'nu etkinleştirdikten sonra, 'Başkalarının kullandığı uygulamalar'ın altındaki ayarları kontrol edin. Bu ayarlar, arkadaşlarınızın kullandığı uygulamalardan bazı kişisel verilerinizi saklayabilmenizi sağlar. Ne yazık ki, **Facebook** bütün kişisel bilgilerinizi saklamanıza izin vermez. Bazı bilgi kategorileri (arkadaş listeniz, cinsiyetiniz ve kamuya açık hale getirdiğiniz bilgiler gibi), **Facebook** 'uygulama Platformu' 'açık' olduğu sürece görünür hale gelir. Bu durumun güvenliğinizi için ne derece önemli olduğuna karar vermek size kalmıştır.

Şimdi **Facebook** hesabınızı **Jitsi'ye** eklemeye hazır hale geldiniz. Bunu yapmak için aşağıdaki adımları takip ediniz:

**1. Adım.** Ana menüden **Dosya – Yeni hesap ekle...**'yi seçin

**2. Adım.** Yeni Hesap Ekle diyalogunda **Ağ** menüsünden **Facebook'u** seçin. **Kullanıcı adı ve parolanızı** **girin** ve **'Ekle'yi** **tıklayın**.

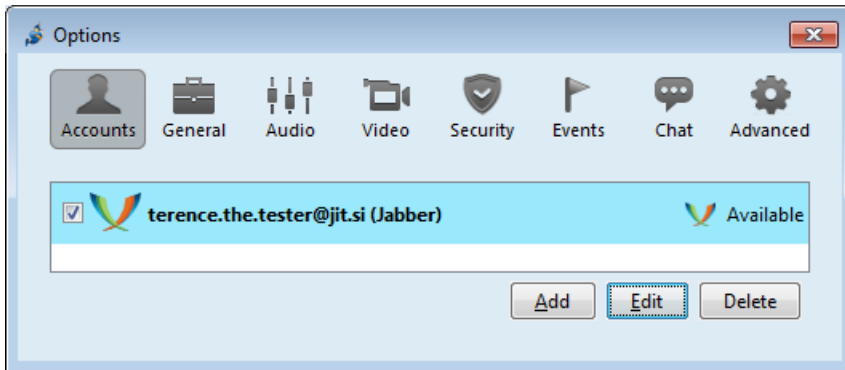


Şekil 10: Facebook hesabı için 'Yeni Hesap Ekle' penceresi örneği

## 2.3 Jitsi ile nasıl hesap parolası değiştirilir?

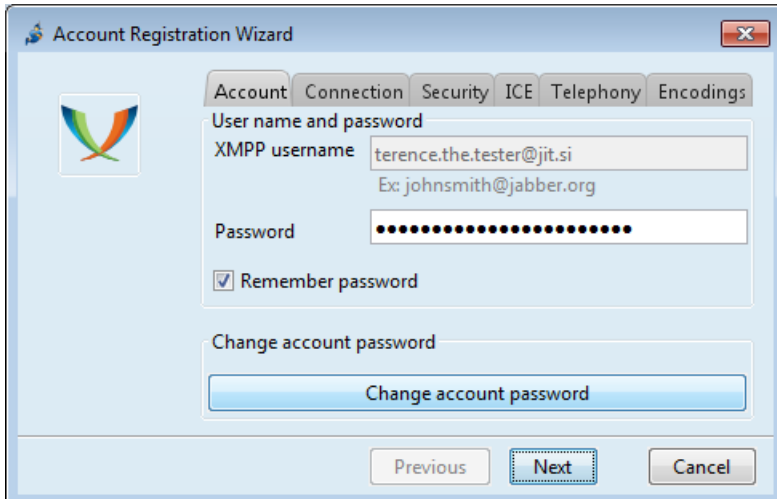
Kişinin sahip olduğu her hesabın parolasını nasıl değiştireceğini bilmesi güvenlik açısından önemli bir konudur. Jitsi ile kullanabileceğiniz hesapların bir çoğunun ayarlarının içinde parola değiştirme seçeneği vardır ve bunlar web ara yüzü üzerinden erişilebilirlerdir. Fakat, bazı Jabber/XMPP ve SIP hesaplarının bu ayarlara ulaşabilecek web arayüzleri yoktur. Bu durumlarda, Jitsi kullanarak parolanızı değiştirmek için aşağıdaki adımları takip edebilirsiniz:

**1. Adım.** Menüden **Araçlar > Seçenekler'i** seçin ve **Hesaplar** sekmesini seçin



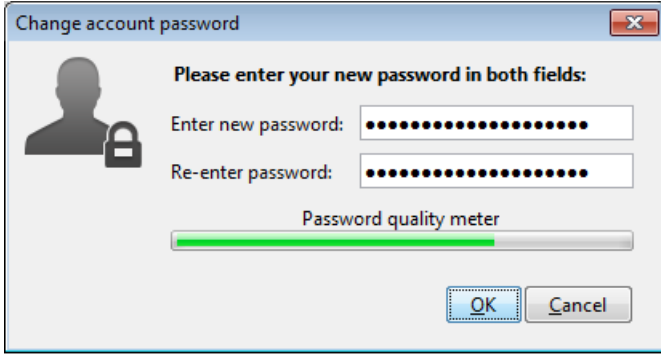
Şekil 11: Bir hesap seçili Seçenekler penceresi

**2. Adım.** Aşağıda görünen pencereyi etkinleştirmek için alt kısımdaki **Düzenle'yi** tıklayın:



Şekil 12: Alt kısımda Hesap parolanızı değiştirin seçeneği ile birlikte Hesap Kayıt Sihirbazı

**3. Adım.** Hesap parolası değiştirme penceresini etkinleştirmek için **Hesap Parolası Değiştir'i** tıklayın:



Şekil 13: Hesap parolası değiştirme penceresi

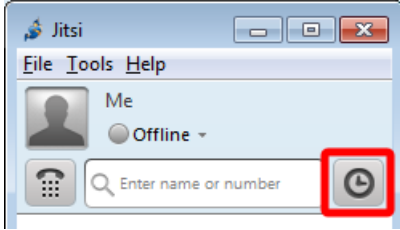
**4. Adım. Yeni parolanızı girin ve yeniden girin.** Bu pencereyi kapatmak için **OK'yi** tıklayın.

**5. Adım.** Hesap Kayıt Sihirbazını kapatın.

## 2.4 Güvenliğini arttırmak için Jitsi nasıl yapılandırılır?

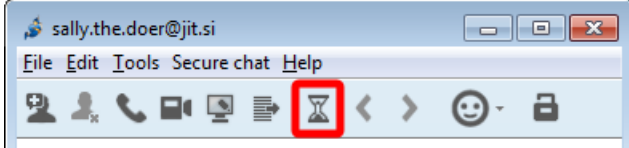
### 2.4.1 Arama ve sohbet geçmişini devre dışı bırakma ve silme

**Jitsi** verili olarak gelen ve giden ses/video arama bilgilerini ve yazılı sohbetlerinizin (gönderdiğiniz ve size gelen tüm mesajlar) tarihini kayıt altına alır. Ses/video aramalarına ana Jitsi penceresindeki saat ikonunu **tıklayarak** ulaşabilirsiniz:



Şekil 14: Arama geçmişi düğmesi işaretli Jitsi ana penceresinin üst kısmı

Birisi ile sohbet ederken yazılı sohbet penceresindeki kum saatine **tıklayarak** sohbet tarihinizi görebilirsiniz



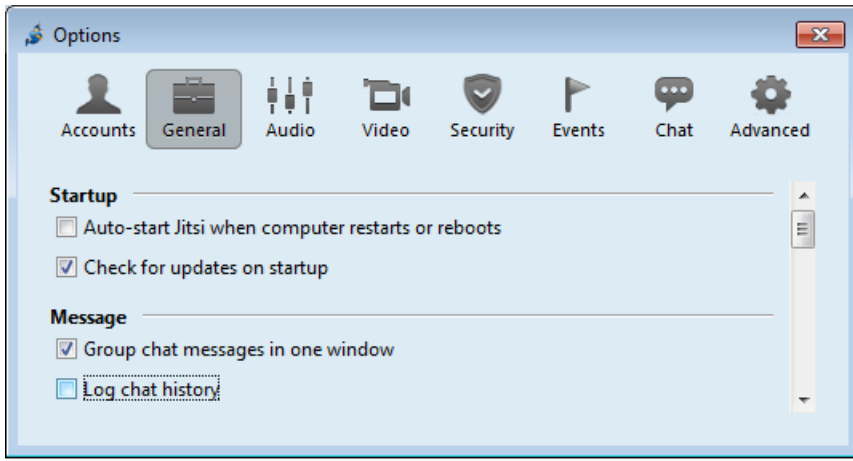
Şekil 15: Sohbet geçmişi işaretli Sohbet penceresi

Bu bilgiler bilgisayarınızın diskinde toplanır ve saklanır. **Yazılı sohbetinizi OTR kullanarak şifrelemiş olsanız bile, gönderdiğiniz ve aldığınız tüm yazılı mesajlar bilgisayarınızda açık metin formatında saklanır.** Aynı bilgiler sohbet ettiğiniz kişilerin bilgisayarlarında da kayıt altına alınır.

Jitsi'nin bu bilgileri toplamasını engellemek için (ve hali hazırda saklanmış olan bilgileri silmek için), **siz ve temas halinde olduğunuz kişiler aşağıdaki adımları takip etmelidir.**

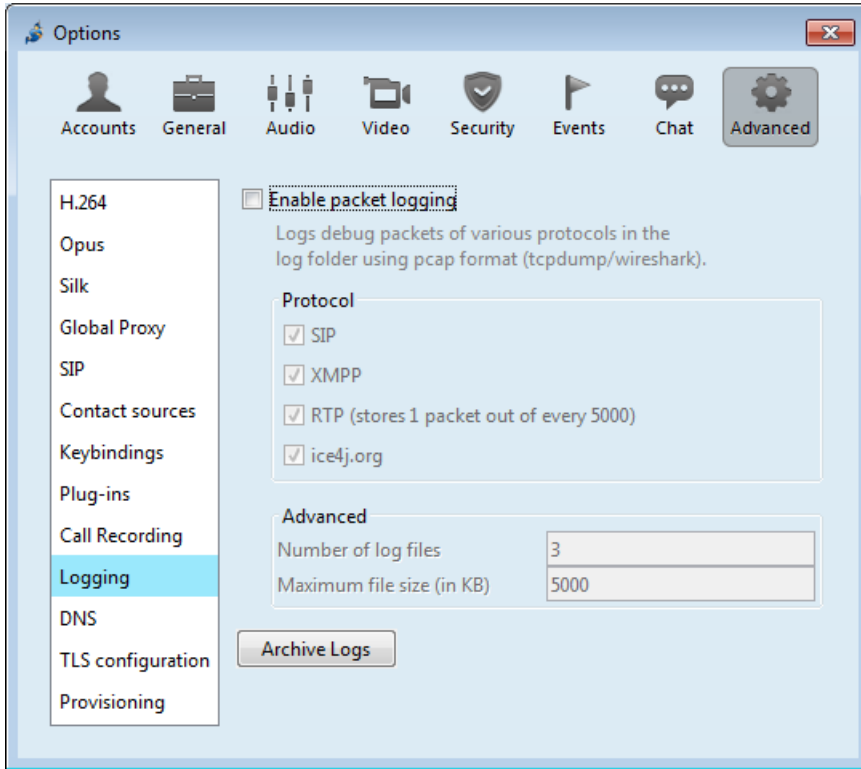
**Jitsi'nin bu bilgileri toplamasını engellemek için:**

**1. Adım.** Menüden **Araçlar > Seçenekler'i** seçin. **Genel** sekmesini **seçin** ve **Sohbet geçmişi kaydet** seçeneğinin işaretini aşağıda görüldüğü gibi **kaldırın**:



Şekil 16: 'Seçenekler' penceresi, 'Genel' sekmesi ve işareti kaldırılmış 'Sohbet geçmişini kaydet'

**2. Adım.** Seçenekler penceresinde, önce **Gelişmiş** sekmesini **seçin**, daha sonra **Kayıt** bölümünü **seçin** ve **Paket girişini etkinleştir** seçeneğinin aşağıda görüldüğü gibi **işaretini kaldırın**:



Şekil 17: 'Seçenekler' penceresinde, 'Gelişmiş' sekmesi, Paket kaydını etkinleştir işareti kaldırılmış durumda

Yaptığınız değişiklikler, **Jitsi**'yi yeniden başlattığınızda etkinleşecektir. .

**Hali hazırda kaydedilmiş olan arama ve yazılı mesaj bilgilerinizi silmek için:**

**1. Adım.** Jitsi'yi kapatın.

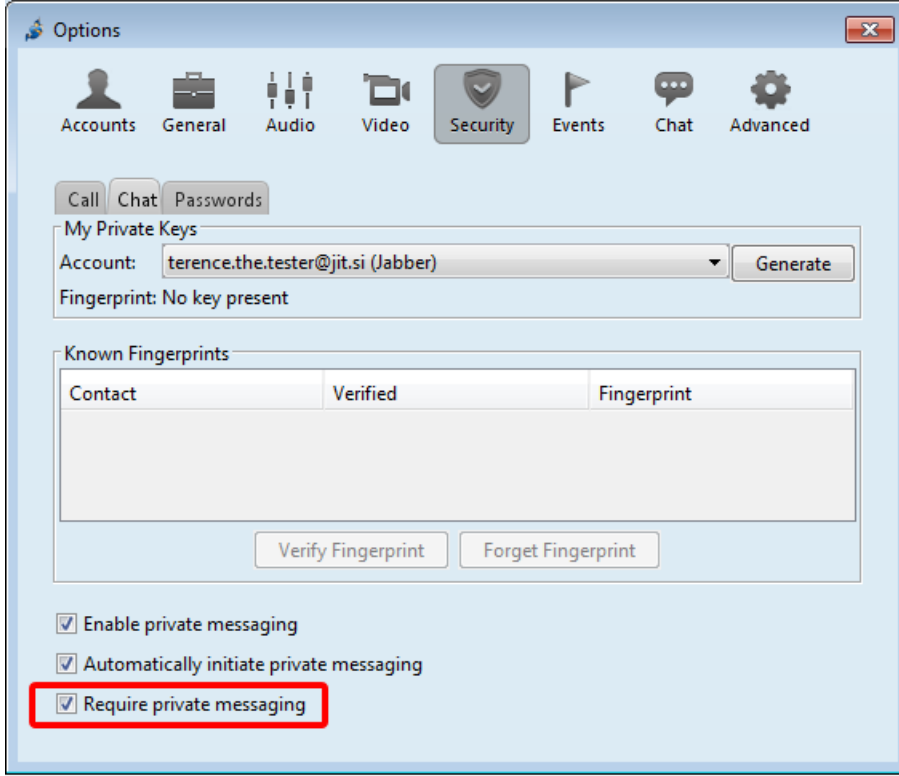
**2. Adım.** *history\_ver1.0* adındaki geçmiş klasörünün tümünü, **Jitsi kullanıcı profili** klasöründen silin. İsterseniz *history\_ver1.0* klasörünün alt-klasörlerinden birini de silebilirsiniz. *Kullanıcı profili* ve *kayıt tarihi* klasörlerinin konumu işletim sistemine göre değişir:

- Windows XP ve önceki versiyonlarında bulunduğu yer: *C:\Belgeler ve Ayarlar\Uygulama Verileri\Jitsi\tarih\_ver1.0*
- Windows Vista, 7, 8'de bulunduğu yer: *C:\Kullanıcılar\<<Windows giriş/kullanıcı adı>\UygulamaVerileri\Gezici\Jitsi\tarih\_ver1.0* ('Uygulama Verileri' dosyası saklı olabilir. [Saklı dosyaları nasıl göreceğiniz ile ilgili bilgi için buraya bakınız](#) <sup>[153]</sup>)
- Mac OS X'te bulunduğu yer: ana klasörden *~/Kütüphane/Uygulama Destek/Jitsi/tarih\_ver1.0*
- Linux'ta bulunduğu yer: ana klasörden *~/jitsi/tarih\_ver1.0* (**Not:** 'jitsi' klasörü saklı olabilir. *Ubuntu*'daki gizli klasörleri [nasıl göreceğiniz ile ilgili bilgi için buraya bakınız](#) <sup>[154]</sup>).

Bilgileri güvenli bir şekilde imha için [Hassas bilgiler nasıl imha edilir](#) <sup>[59]</sup> bölümüne de bakabilirsiniz.

## 2.4.2 Yazılı sohbette özel mesaj şartı

Jitsi'yi OTR <sup>[155]</sup> şifrelemesi <sup>[156]</sup> kullanarak gizli ve şifrelenmiş yazılı mesajlaşma uygulayacak şekilde kurmanızı tavsiye ederiz. Bunu yapmak için, menüden **Araçlar > Seçenekler'i seçin**, **Güvenlik** seçmesini **seçin**, **Sohbet** alt-sekmesini **seçin** ve ekranın altındaki **Özel mesajlaşma şartı koy** seçeneğini aşağıda görüldüğü şekilde **işaretleyin**:



Şekil 18: 'Özel mesajlaşma şartı koy' seçili, 'Seçenekler' penceresi, 'Güvenlik' sekmesi 'Sohbet' alt-sekmesi

### 2.4.3 Ana parola ile hesaplarınızın parolalarını koruma

Jitsi'nin hesaplarınızın parolalarını hatırlamasına izin vermemek en iyisidir. Kullanım kolaylığı açısından tersini yaparsanız, bilgisayarınızı kullanan herhangi biri Jitsi'yi başlatarak tüm hesaplarınıza giriş yapabilir. Aynı zamanda, *Seçenekler* penceresinde parolalarınızı görebilir. Bu yüzden, hesap parolalarınızı güçlü bir **ana parola** ile korumanızı **şiddetle tavsiye ederiz**. Ana parolayı oluşturulunca, Jitsi her başlatıldığında size bu parolayı soracaktır.

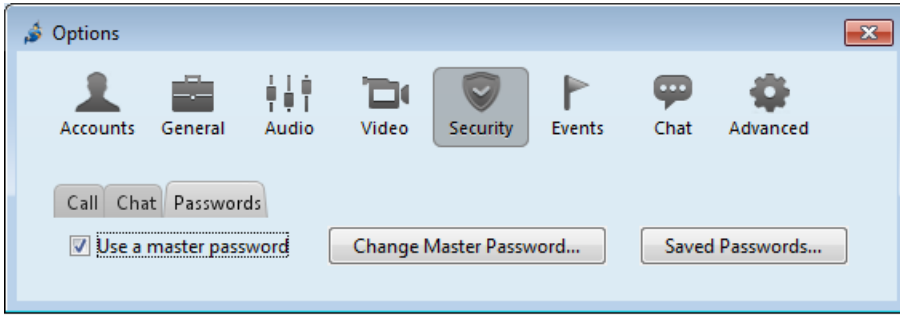
**1. Adım.** Menüden **Araçlar > Seçenekler'i** seçerek *Seçenekler* penceresini **açın**, **Güvenlik** sekmesini **seçin**, **Parolalar** alt-sekmesini **seçin** ve **Ana Parola** penceresini etkinleştirmek için **Ana parola Kullan'ı işaretleyin**.

**2. Adım.** Aşağıdaki resimde görüldüğü gibi, açılan pencereye **parolanızı girin**. Güçlü parolalar oluşturmak konusunda daha fazla bilgi için, **Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** <sup>[157]</sup> bölümüne bakın.



Şekil 19: 'Ana Parola' penceresi

**3. Adım.** Parolayı onaylamak için **'OK'i** tıklayın ve **Ana Parola başarılı bir şekilde oluşturuldu** yazısını içeren pencereyi etkinleştirin. Pencereyi kapatmak için **'OK'i** tıklayın ve *Seçenekler* penceresine geri dönün. Bu pencere aşağıdaki gibi görünecektir:



Şekil 20: 'Seçenekler' penceresi, 'Güvenlik' sekmesi, 'Parolalar' alt-sekmesi, 'Ana parola kullan' seçeneği işaretli

**Not: Ana Parolayı Değiştir** düğmesi ana parolayı değiştirmenize izin verir, **Kaydedilen Parolalar...** düğmesi Jitsi tarafından hatırlanan parolalara erişmenizi ve gerektiği zaman onları silmenizi sağlar.

## Jitsi – Kişi ekleme ve yazılı ve sesli iletişim kurma

Bu sayfadaki bölümlerin listesi:

- **3.1 Jitsi'ye kişi (arkadaş) ekleme**
- **3.2 OTR şifreleme ile yazılı sohbet (Anlık Mesajlaşma)**
- **3.3 ZRTP şifreleme ile sesli ve görüntülü sohbet**

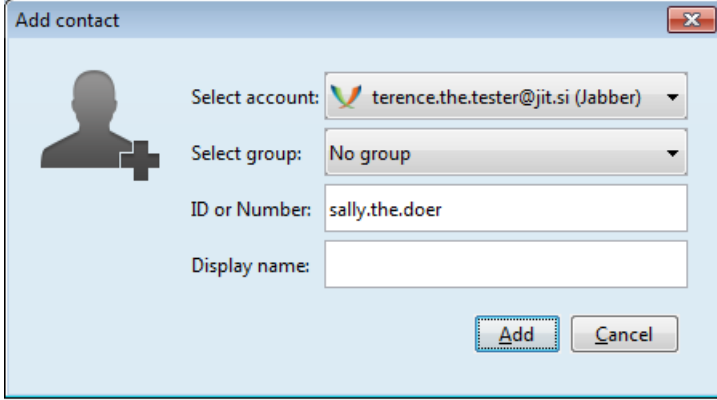
### 3.1 Jitsi'ye kişi (arkadaş) ekleme

Jitsi'ye bir hesap ekledikten ve giriş yaptıktan sonra, daha fazla kişi eklemeye ve onlarla iletişim kurmaya hazırsınız.

Jitsi'ye bir kontakt eklemek için aşağıdaki adımları takip ediniz:

**0. Adım. Başla > Jitsi'yi seçerek** veya masaüstündeki **Jitsi** ikonuna **çift tıklayarak** Jitsi ana penceresin açın.

**1. Adım. Dosya > Kontakt ekle...'**yi seçin ve aşağıda görünen pencereyi açın:



Şekil 1: Kontakt ekle penceresi

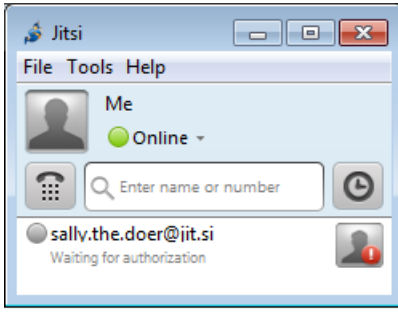
**2. Adım.** Kişiyi hangi hesabınıza eklemek istediğinizi **seçin** (örneğin, erance.the.test@jit.si).

**İsteğe bağlı:** Kişiyi belli arkadaşlarınızdan oluşan bir *gruba* da ekleyebilirsiniz. Fakat önce bu grubu oluşturmalısınız. Bunu menüden **Dosya – Grup oluştur...'**u seçerek yapabilirsiniz.

**Kimlik veya Numara** alanına kişinin kullanıcı adı veya adresini **yazın** (örneğin, sally.the.doer@jit.si).

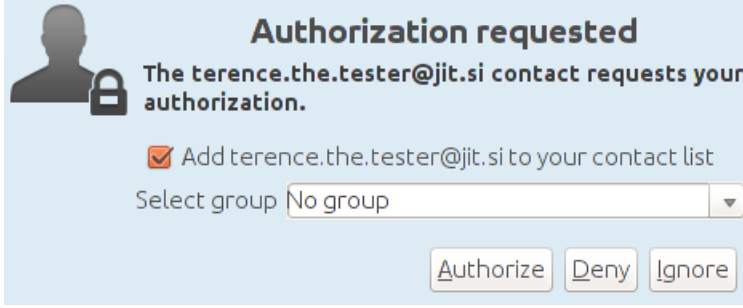
Kişi için, **Jitsi** ana penceresindeki arkadaş listenizde görünecek bir isim veya rumuz seçebilirsiniz. Bunu **Görünen isim** alanına **yazabilirsiniz**.

**3. Adım.** *Kişi ekleme* penceresini kapatmak ve Jitsi ana sayfasına geri dönmek için *Ekle'yi tıklayın*. Arkadaş listenizde yeni eklenen kişileri, 'kimlik doğrulama bekleniyor' notu ile birlikte, aşağıdaki gibi göreceksiniz:



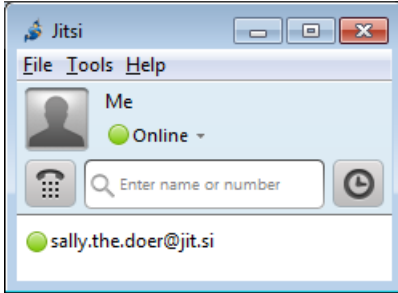
Şekil 2: Kimlik doğrulama bekleyen yeni eklenmiş kişileri gösteren Jitsi ana sayfası

**4. Adım.** Eklediğiniz kişi (sally.the.doer@jit.si) kendi hesabına giriş yaptığı zaman onu arkadaş listenize eklemek istediğinizi söyleyen açılır bir pencere ile karşılaşacak.



Şekil 3: Yeni eklenen kişiye kimlik doğrulama isteği gönderen pencere

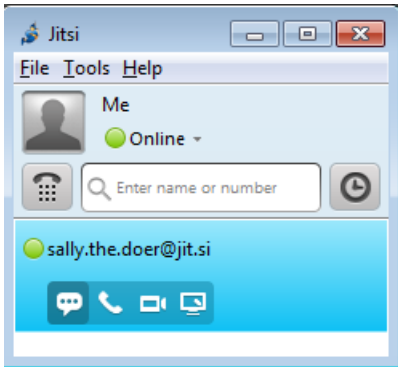
Eklediğiniz kişi, Yoksay'ı seçebilir, bu durumda gönderdiğiniz istek yetkilendirilmeyi beklemeye devam edecektir. Bunu yapması halinde, isteğinizin reddedildiğine dair bilgi alacaksınız. 'Doğrulama'yı seçerse, eklediğiniz kişinin yetkilendirme isteğini kabul ettiğine dair bilgi alacaksınız ve kişi arkadaş listenizde aktif hale gelecek:



Şekil 4: Yetkilendirilmiş yeni kişiyi gösteren Jitsi ana penceresi

## 3.2 OTR şifreleme ile yazılı sohbet (Anlık Mesajlaşma)

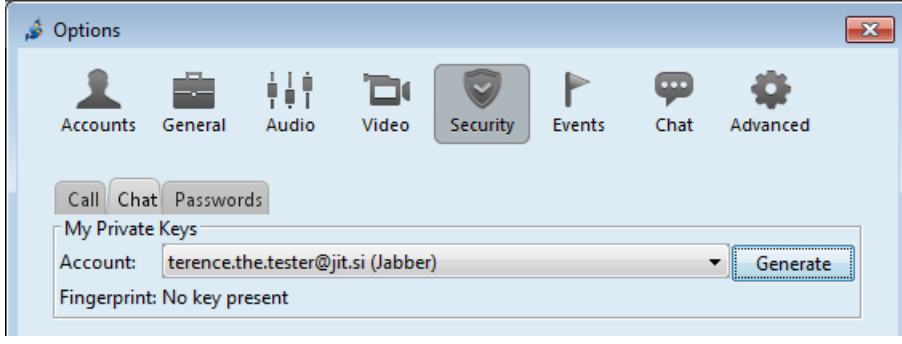
Kişiyi ekleyip kimlik doğruladıktan sonra arkadaş listenizde isminin üzerine tıklayıp yazılı, sesli veya görüntülü sohbet başlatabilir, isminin altındaki uygun ikonu seçerek masaüstü paylaşımında bulunabilirsiniz:



Şekil 5: Jitsi ana sayfasında seçili kişiler ve yazılı, sesli veya görüntülü sohbet ve masaüstü paylaşımı ikonları

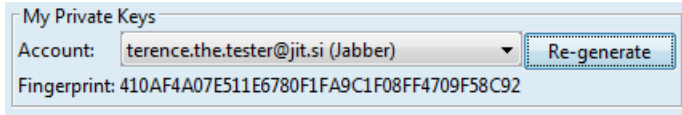
**1. Adım.** Şimdi Jitsi'nin en önemli özelliklerinden bir tanesine değineceğiz: mesajlarınızı OTR <sup>[129]</sup> kullanarak şifreleme ve böylelikle güvenli bir şekilde yazılı sohbet etme. OTR, bu kılavuzdaki diğer bölümlerde incelenmiş olan GPG/PGP <sup>[158]</sup>'ye benzer bir şekilde çalışır. Aynı PGP gibi, hem sizin hem de iletişim halinde olduğunuz kişinin iletişiminizi şifrelemeden önce, şifreleme anahtarlarınızı oluşturmak için **Jitsi'yi** yapılandırmanız gerekir. Bunu, menüden **Araçlar > Seçenekler'i**

**seçerek** yapabilirsiniz. Ardından, **Güvenlik** sekmesini ve **Sohbet** alt-sekmesini **seçin**. Aşağıda görüneceği bir pencere ile karşılaşacaksınız:



Şekil 6: Yazılı sohbetleriniz için şifreli anahtarlar oluşturabileceğiniz sohbet seçenekleri penceresinin bir kısmı

**2. Adım. Oluştur** düğmesine **basın**. Oluşturulan anahtarın parmak izini göreceksiniz:

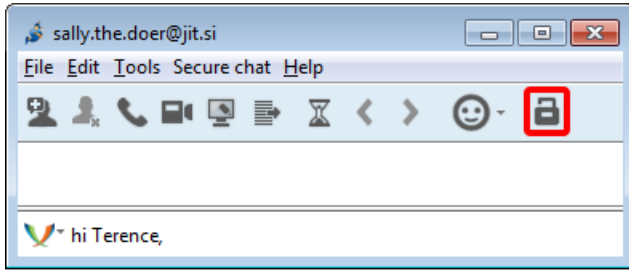


Şekil 7: Oluşturulmuş OTR şifreli yazılı sohbetinizin parmak izini gösteren sohbet seçenekleri penceresinin bir kısmı

Her hesap için bir anahtar oluşturulur. Yeni bir hesap eklediğiniz veya Jitsi'yi başka bir cihaza indirdiğiniz zaman bu işlemi yeniden yapmanız gerekir. Var olan anahtarları oraya taşıyamazsınız.

Şimdi iletişim kurmaya hazırsınız:

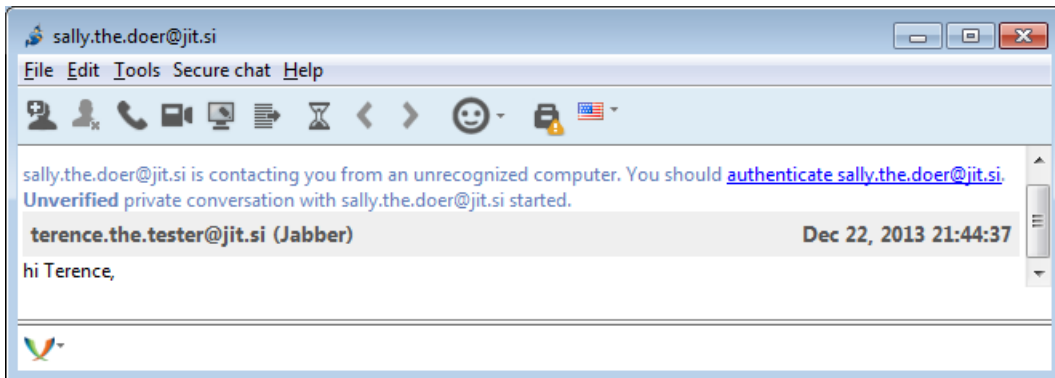
**3. Adım.** Jitsi ana sayfasından bir **kişi seçin** ve **mesaj gönder** ikonunu **tıklayın** (kişinin isminin altındaki soldaki ilk ikon). Aşağıdaki yazılı sohbet penceresi açılacaktır:



Şekil 8: OTR şifrelenmiş yazılı sohbet penceresi, işaretli fakat devreye girmemiş

Pencerenin sağ üst köşesindeki asma kilide ve **Sohbeti OTR ile şifrele** ikonuna dikkat ediniz. Çok kolay göze çarpmayan bu ikon sohbetin şifreli olup olmadığı konusunda bilgi verir. Resimdeki anahtar açık (kilidin gövdesi ve kolu arasında çok küçük bir boşluk var!).

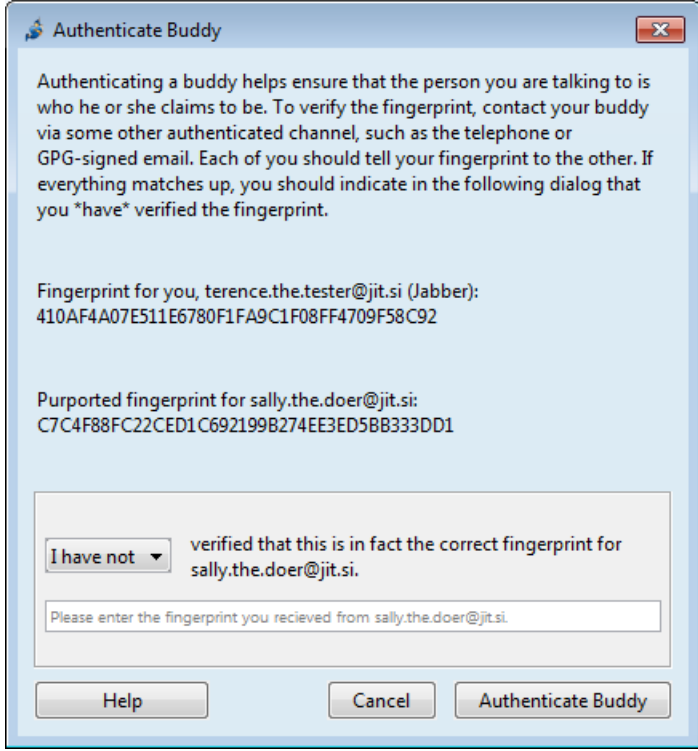
**4. Adım. Sohbeti OTR ile şifrele** ikonunu **tıklayın**. Pencerede olan değişikliklere dikkat edin



Şekil 9: Sohbeti OTR ile şifrele ikonunu tıkladıktan sonra yazılı sohbet penceresi

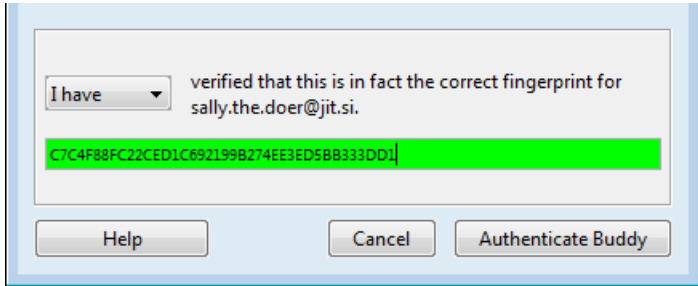
Asma kilidin şimdi kapalı olduğunu görebilirsiniz. Bu, iletişim kurduğunuz kişi ile birbirinize gönderdiğiniz mesajların şifreli olduğu anlamına gelir. Bunun *onaylanmamış gizli bir iletişim* olduğuna dair bir mesaj alacaksınız, sally.the.doer@jit.si'nin kimliğini doğrulamanız gerekir

5. Adım. **sally.the.doer@jit.si'nin kimliğini doğrulamanız** için **bağlantıya tıklayın** ve **Arkadaşının Kimliğini Doğrula** penceresini açın:



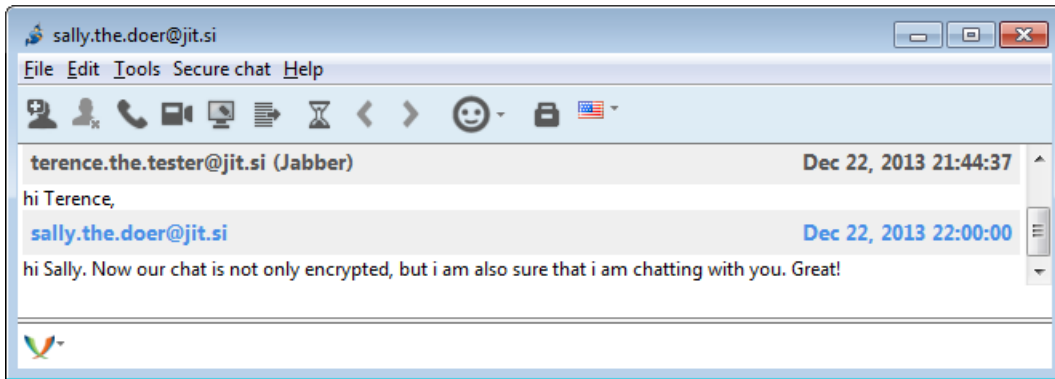
Şekil 10: Siz ve iletişimde olduğunuz kişinin parmak izlerini gösteren Arkadaşının Kimliğini Doğrula penceresi

İletişimde olduğunuz kişi ile anahtarlarınızın parmak izlerini, bu yazılı sohbet dışındaki başka bir kanal üzerinden karşılaştırmayı isteyen mesaja dikkat edin. Bunu yaparak, iletişim kurduğunuz kişinin gerçekten o olduğundan emin olabilirsiniz. Anahtar karşılaştırması yapmak için en iyi yöntem yüz yüze olmak ya da görüntülü veya sesli iletişim kurmaktır. Bu yöntemlerle karşınızdaki kişinin kimliğini doğrulamak daha kolaydır. Parmak izlerini karşılaştırdıktan sonra, aşağı açılır menüden **Parmak izini doğruladım** seçeneğini **seçin** ve **Arkadaşının Kimliğini Doğrula'yı** tıklayın:



Şekil 11: Parmak izini 'doğruluyorum' seçeneğini seçtikten sonra Arkadaşın Kimliğini Doğrula penceresinin bir kısmı

**Arkadaşını Doğrula** penceresini kapatmak sizi sohbet penceresine götürecektir:



Şekil 12: Doğrulanmış OTR şifreleme ile Yazılı sohbet penceresi

Asma kilidin artık beyaz ünlem işareti içeren turuncu üçgeni göstermediğini görebilirsiniz. Bu arkadaşınızın kimliğiniz doğruladığınız anlamına gelir. **Kimlik doğrulama her kişi için bir kere yapılmalıdır.** Ünlem işaretli üçgen yeniden belirirse, kimliğini doğrulamadığınız birisi ile sohbet ediyorsunuz demektir. Bu, arkadaşınız başka bir şifrelenmiş anahtar ile (farklı bir Jitsi kurulumu veya OTR tarafından etkin kılınmış başka bir program) farklı bir cihaz kullandığında gerçekleşebilir.

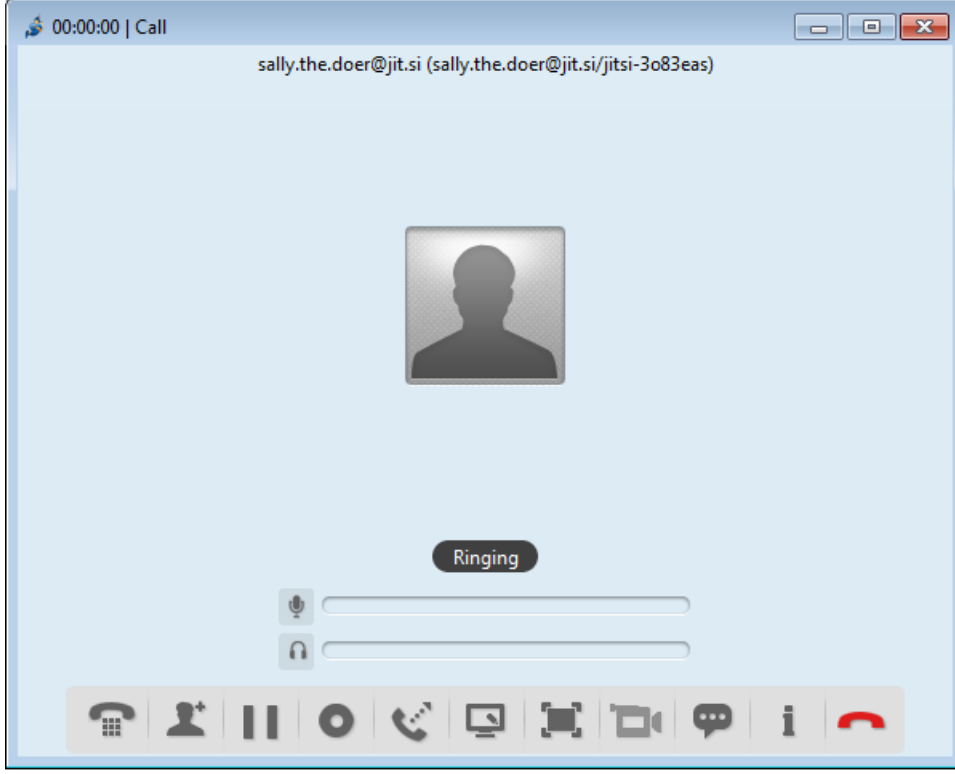
Bu durumda, iletişim kurduğunuz kişinin kimliğinden emin olmak için birbirinizin kimliklerini yeniden doğrulamanız gerekir.

**Jitsi** aynı anda birden fazla kişi ile sohbet etmenize olanak sağlar. OTR şifreleme ise bir kişi ile sohbet ederken çalışır.

### 3.3 ZRTP şifreleme ile sesli ve görüntülü sohbet

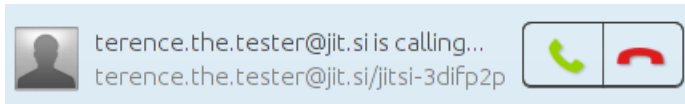
**Jitsi**, ZRTP adlı açık bir standart tarafından bağımsız olarak şifrelenebilen sesli ve görüntülü sohbet imkanı sağlar. Oturumu açmak için:

**1. Adım. Jitsi** iletişim listesinden iletişim kuracağınız kişiye **tıklayın** ve ses (kişinin isminin altındaki soldan ikinci ikon) veya video (üçüncü) ikona tıklayın. Yukarıdaki Şekil 5 bunu nasıl yapacağınızı gösterir. **Jitsi'nin** bağlantıyı kurduğunu gösteren yeni bir pencere açılacaktır:



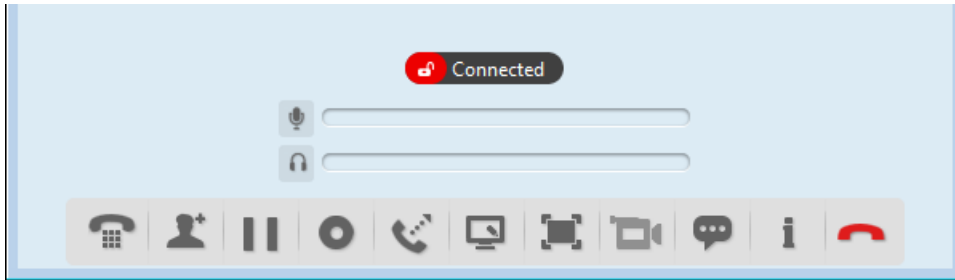
Şekil 13: Çalma statüsü belirten arama penceresi

İletişim kurduğunuz kişi gelen arama bildirimini görecektir:



Şekil 14: Gelen arama bildirimi

**2. Adım.** Arkadaşınız **aramayı kabul ederse** bağlantı kurduğunuza dair bilgilendirileceksiniz:

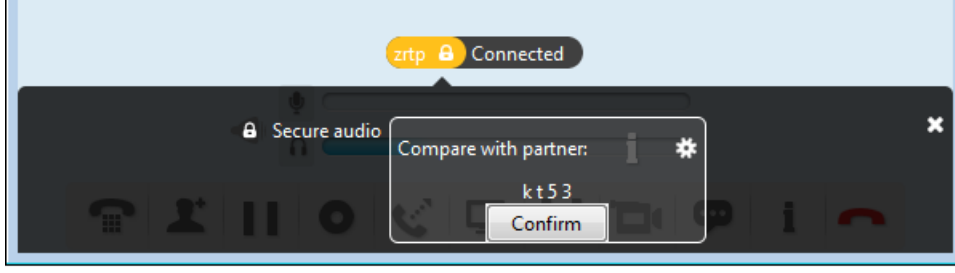


Şekil 15: ZRTP şifrelemesiz gelen arama penceresi

Kırmızı asma kilidin açık olduğunu görebilirsiniz. Bu, aramanızın henüz ZRTP ile şifrelenmemiş olduğunu gösterir.

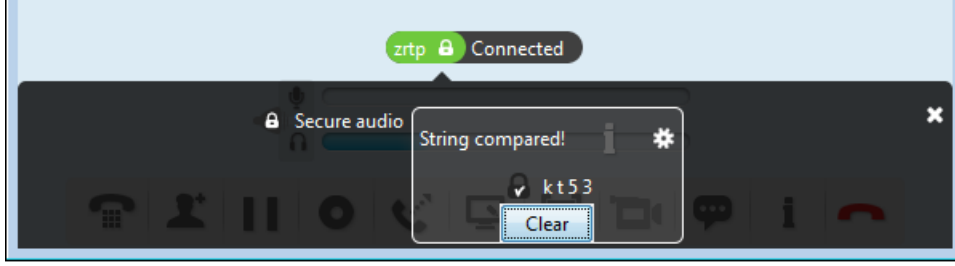
**3. Adım. Bekle...** Sizin ve iletişim kurduğunuz kişinin programlarının şifrelenmiş bir bağlantı kurması bir süre alabilir. Bu işlem başarı ile gerçekleşirse, turuncu bir arka planda, aşağıda görüldüğü gibi kapalı bir asma kilit ile birlikte **zrtp** harflerini göreceksiniz. Bu bağlantıyı kurmayı başaramazlarsa, sohbet etmeye devam edebilirsiniz, fakat sohbetiniz şifrelenmemiş olur. Bağlantıyı kesip **Jitsi'yi** yeniden başlatabilir ve programların şifreli bir bağlantı kurmayı yeniden denemesine izin

verebilirsiniz. Farklı sunuculara sahip (Google ve Jit.si gibi) hesaplar arasındaki aramalarda ZRTP'nin çalışmama olasılığı vardır.



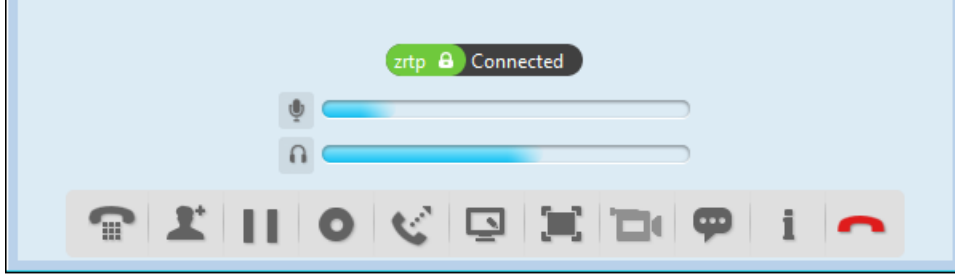
Şekil 16: Etkinleşmiş fakat doğrulanmamış ZRTP şifreleme ile Arama penceresinin bir kısmı

**4. Adım.** *zrtp* harflerinin ve asma kilidin altındaki kısımda 'Partneriniz ile kıyaslayın' yazan ve 4 karakter ile devam eden bir mesaj **göreceksiniz**. Bu harfleri iletişimde olduğunuz kişiye **okuyun** ve onda da aynı karakterlerin olup olmadığını sorun. Eğer varsa iletişiminiz şifrelenmiş demektir ve kimse bu iletişime dahil olamaz. **Onayla'yı tıklayabilirsiniz**. Turuncu *zrtp* alanı yeşile dönecektir:



Şekil 17: Devreye girmiş ve onaylanmış ZRTP şifrelemesi ile Arama ekranının bir kısmı

**5. Adım.** Siyah kısmın sağ üst köşesindeki beyaz x işaretine tıklayarak pencerenin siyah onaylama kısmını kapatabilirsiniz:



Şekil 18: Devreye girmiş ve onaylanmış ZRTP şifrelemesi ile Arama ekranının bir kısmı

**Jitsi**, birden fazla kişi ile sesli ve görüntülü sohbet etmenize olanak sağlar. Dikkat edin ki bu tür iletişim esnasında, ZRTP şifreleme, aramayı başlatan kişi ve diğer taraflar arasında devreye girebilir, diğer katılımcıların kendi aralarında değil.

## Thunderbird, Enigmail ve GPG ile - Güvenli E-posta İstemcisi

### Short Description:

**Mozilla Thunderbird** e-postaları almak, yollamak ve de saklamak için kullanılan ücretsiz ve açık-kaynak olan bir e-posta istemcisidir. **Enigmail** ve **GnuPG** size kimlik doğrulama, digital imza, şifreleme imkanı vererek gizliliğinizin ve güvenliğinizin korunmasını sağlar.

### Online Installation Instructions:

#### Thunderbird, Enigma ve GnuPG'yi indirme

- Kısa **Uygulamalı Rehber'in** <sup>[1]</sup> Giriş bölümünü **okuyun**
- Aşağıdaki **Thunderbird** ikonunu **tıklayarak** [www.mozilla.org/tr/thunderbird/](http://www.mozilla.org/tr/thunderbird/) sayfasını açın
- **Ücretsiz indirin** linkini **tıklayarak** yükleme dosyasını indirin, bu dosyayı **bulup**, üstüne **çift tıklayın**
- Aşağıdaki **Enigmail** ikonunu **tıklayarak** [enigmail.net/download](http://enigmail.net/download) sayfasını açın
- **Download v1.7 for Thunderbird 31** linkine **sağ-tıklayın**, ve eklentiği bilgisayarınıza **kaydedin**
- Aşağıdaki **GnuPG** ikonunu **tıklayarak** [ftp://ftp.gnupg.org/gcrypt/binary/](http://ftp.gnupg.org/gcrypt/binary/) sayfasını açın
- **gnupg-w32cli-1.4.X.exe** isimli (mesela, [gnupg-w32cli-1.4.18.exe](http://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.18.exe) <sup>[159]</sup>) son dosyayı görene kadar **aşağı kaydırın**, buna **tıklayarak** kurulum dosyasını kaydedin

- **Enigmail** ve **GnuPG**'yi kurmak için bu **Thunderbird** rehberinin **4.1 kısmına** devam edin
- Aşağıdaki **TorBirdy** ikonuna **tıklayarak** eklentiye bilgisayarınıza kaydedin
- Kurulumları tamamladıktan sonra bütün kurucu ya da eklentileri bilgisayarınızdan silebilirsiniz

**Thunderbird: Enigmail: GnuPG: TorBirdy:**



## Ana Sayfa

- [www.mozilla.com/thunderbird](http://www.mozilla.com/thunderbird) [164]
- [www.enigmail.net](http://www.enigmail.net) [165]
- [www.gnupg.org](http://www.gnupg.org) [166]
- [trac.torproject.org/projects/tor/wiki/torbirdy](http://trac.torproject.org/projects/tor/wiki/torbirdy) [167]

## Bilgisayar Gereksinimleri

- Bütün Windows Versiyonları

## Bu rehberde kullanılan sürümler

- Thunderbird 31.0
- Enigmail 1.7
- GNU Privacy Guard (GnuPG) 1.4.18
- TorBirdy 0.1.2

## Bu bölümün son güncellenme tarihi

- Eylül 2014

## Lisans

- Ücretsiz ve Açık-Kaynak Yazılım

## Gerekli Okuma

- Nasıl Yapmalı Kitapçığı'nın **7. Bölümü, İnternet iletişiminizin gizliliği nasıl korunur** [51]

## Buradan sağlayacağınız faydalar:

- Bir program aracılığıyla farklı e-posta hesaplarınızı yönetebilme imkanı
- İnternet bağlantısı koptuktan sonra mesajlarınızı okuyabilme ve yenilerini yazabilme imkanı
- E-postalarınızın gizliliğini koruyabilmek için halka açık anahtar şifrelemesini kullanabilme imkanı

## GNU Linux, Mac ve Microsoft Windows'a Uyumlu Diğer Programlar:

**Mozilla Thunderbird** e-posta istemcisi **GNU Linux, Mac OS, Microsoft Windows** ve diğer işletim sistemleri için erişilebilirdir. Dijital güvenliğinizi sağlanması açısından birden fazla e-posta hesabının yönetimi komplike bir iştir, bu yüzden, **Mozilla Thunderbird**'ü kullanmanızı *şiddetle tavsiye ederiz*. Farklı platformlarda çalışabilen, *ücretsiz ve açık-kaynak* olan **Thunderbird**'ün avantajları özellikle **Microsoft** Outlook gibi ticari denklemlere kıyasla çok daha belirgindir. Fakat, yine de **Mozilla Thunderbird** dışında bir program kullanmak istiyorsanız, size aşağıdaki ücretsiz ve açık-kaynak alternatifleri önerebiliriz.

- **GNU Linux** ve **Microsoft Windows** için ulaşılabilir olan **Claws Mail** [168];
- **GNU Linux, Mac OS** ve **Microsoft Windows** için ulaşılabilir olan Sylpheed **Sylpheed** [169];
- **GNU Linux, Mac OS** ve **Microsoft Windows** için ulaşılabilir olan Alpine **Alpine** [170].

**Not:** Thunderbird ile beraber kullanıldığında sağladığı kullanım kolaylığından dolayı **Enigmail/GnuPG** kombinasyonunu tavsiye ediyor olsak da, **pgp4usb** gibi bağımsız şifreleme programlarını da **Thunderbird** eşliğinde kullanabilirsiniz. Kamusal anahtar şifrelemesini kullanan bu diğer metod hakkında bilgi sahibi olabilmek için lütfen **pgp4usb** [171] bölümünü okuyun.

## 1.1 Başlamadan önce bilmeniz gerekenler

**Mozilla Thunderbird** farklı platformlarda çalışan, e-posta alımı gönderimi ve saklanması için kullanılan ücretsiz ve açık-kaynak bir e-posta istemcisidir. Bir internet tarayıcısını kullanmanıza gerek kalmadan e-posta mesajlarınızı indirip yönetmenizi sağlayan bilgisayar programına e-posta istemcisi denir. Tek bir program birden fazla e-posta hesabını yönetmek için kullanılabilir. **Thunderbird**'ü kullanabilmek için bir e-posta adresinizin olması gerekir. Mesela **RiseUp** [172] üzerinden bir e-posta adresi açabilirsiniz.

**Enigmail, Thunderbird** için geliştirilmiş bir eklentidir. Kullanıcılarına **GNU Privacy Guard (GnuPG)** aracılığıyla kimlik denetimi ve şifreleme imkanlarını sağlar.

**GnuPG** e-posta iletişimlerinin gizliliğini ve güvenliğini sağlayan bir halka açık anahtar şifreleme programıdır. Bunu, mesajları şifreleyip deşifreleyen anahtar çiftleri oluşturmanızı ve yönetmenizi mümkün kılarak yapar. **Enigmail**'in çalışabilmesi için, **GnuPG**'nin bu bölümde daha sonra açıklanacağı şekilde bilgisayarınıza kurulması gerekir.

#### Offline Installation Instructions :

#### Thunderbird Kurulumu

- Kısa [Uygulamalı Rehber'in](#) <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Thunderbird** ikonunu **tıklayıp** kurucuyu 'Açın' ya da 'Çalıştırın'. Kurucuyu önce bilgisayarınıza indirmeniz gerekirse, indirme bittikten sonra yerini bulup üstüne çift tıklayın
- **Enigmail** ikonunu **tıklayıp** eklentiye kaydedin
- **GnuPG** ikonunu **tıklayıp** yükleyiciyi kaydedin
- Rehberi takip etmeye devam edin ve Bölüm 4.1'e ulaştığınızda Enigmail ve GnuPG'yi kurun.
- Kurulumları tamamladıktan sonra bütün kurulum ya da eklentileri bilgisayarınızdan silebilirsiniz

Thunderbird: Enigmail: GnuPG: TorBirdy:



## Thunderbird Nasıl Kurulur?

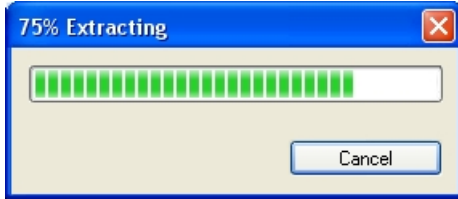
Bu sayfadaki kısımların listesi:

- [2.0 Thunderbird Nasıl Kurulur?](#)
- [2.1 Thunderbird'de Global Arama ve Dizin Oluşturma Nasıl Kapatılır?](#)
- [2.2 Thunderbird'de Bir E-Posta Hesabı Nasıl Kaydedilir?](#)
- [2.3 Thunderbird'de Bloglar, Haber Akışları ve Haber Grupları Nasıl Kaydedilir?](#)

## 2.0 Thunderbird Nasıl Kurulur?

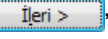
Thunderbird'ü kurmaya başlamak için aşağıdaki adımları takip edin:

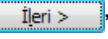
**1. Adım:**  Thunderbird Setup 31.5.0 dosyasına **çift tıklayın**. Dosyayı Aç- Güvenlik Uyarısı kutusu açılırsa, **Çalıştır** 'ı (Çalıştır) **tıklayarak** şu ekranı etkinleştirin:

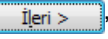


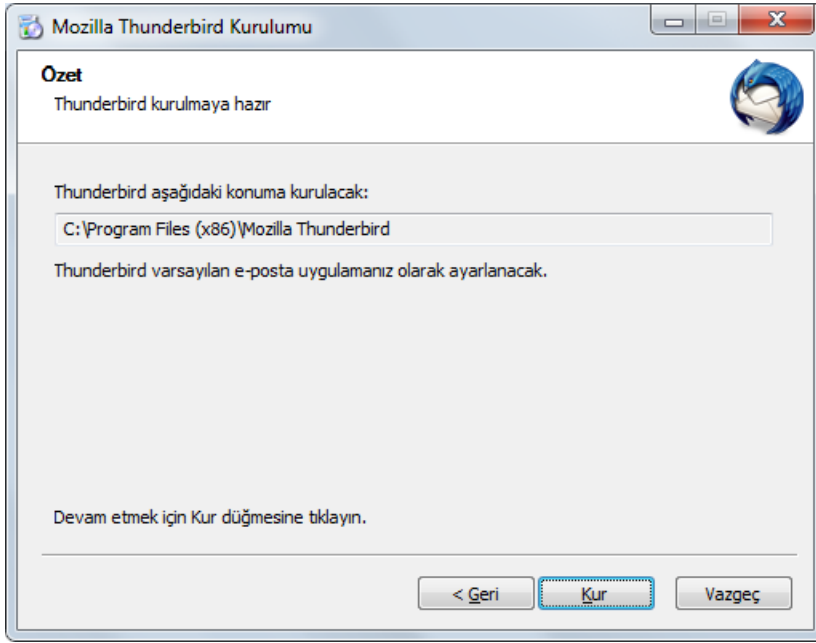
Şekil 1: Çıkarma işlemi statüsü barı

**Thunderbird** dosyalarının çıkartılması tamamlandıktan sonra *Mozilla Thunderbird Kurulum Sihirbazı'na Hoşgeldiniz* ekranı belirir.

**2. Adım:**  'yı **tıklayarak** Mozilla Thunderbird – Kurulum Türü ekranını açın.

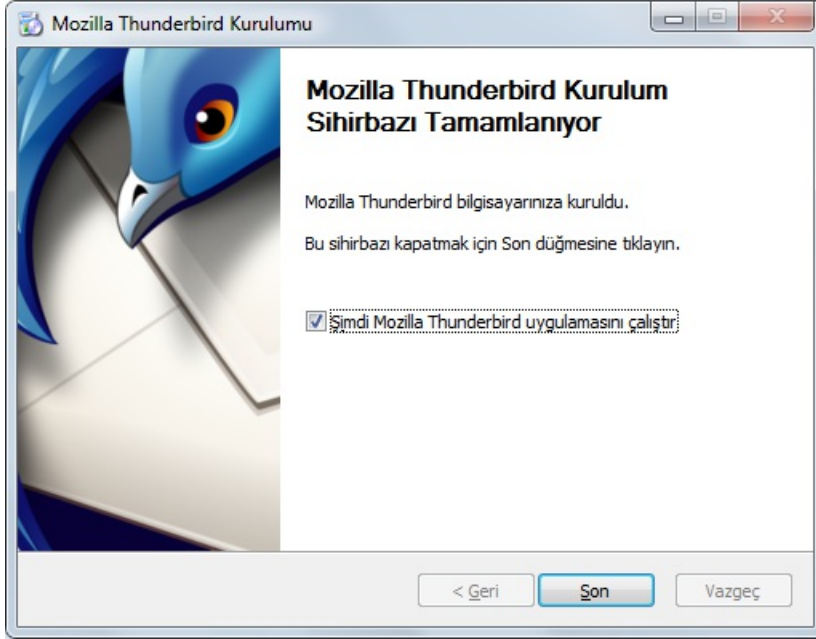
**3. Adım:**  'yı **tıklayarak** Kurulum Seçenekleri sayfasını açın. Siz bir diğerini seçmezseniz Standart kurulum uygulanmaya başlayacak.

**4. Adım:**  'yı **tıklayarak** verili olan kurulum seçeneklerini kabul edin, böylece şu ekranı etkinleştireceksiniz.



Şekil 2: Mozilla Thunderbird - Özet sayfası

5. Adım: **Kur** butonunu tıklayarak kurma işlemini başlatın. Kurma işlemi bitince aşağıdaki ekran belirecek:



Şekil 3: Mozilla Thunderbird Kurulum Sihirbazı Tamamlanıyor ekranı

6. Adım: **Son** butonunu tıklayarak kurulum işlemini bitirin.

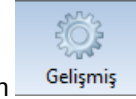
**İpucu:** Eğer yukarıdaki Şekil 3'te gösterildiği gibi Thunderbird'ü şimdi başlat kutusu etkinse, Thunderbird kendiliğinden çalışmaya başlayacaktır. Thunderbird'ü gelecekte açmak için masa üstündeki Thunderbird ikonuna çift tıklayabilirsiniz, ya da, Programlar>Mozilla Thunderbird>Mozilla Thunderbird'ü seçebilirsiniz.

## 2.1 Thunderbird'de Global Arama ve Dizin Oluşturma Nasıl Kapatılır?

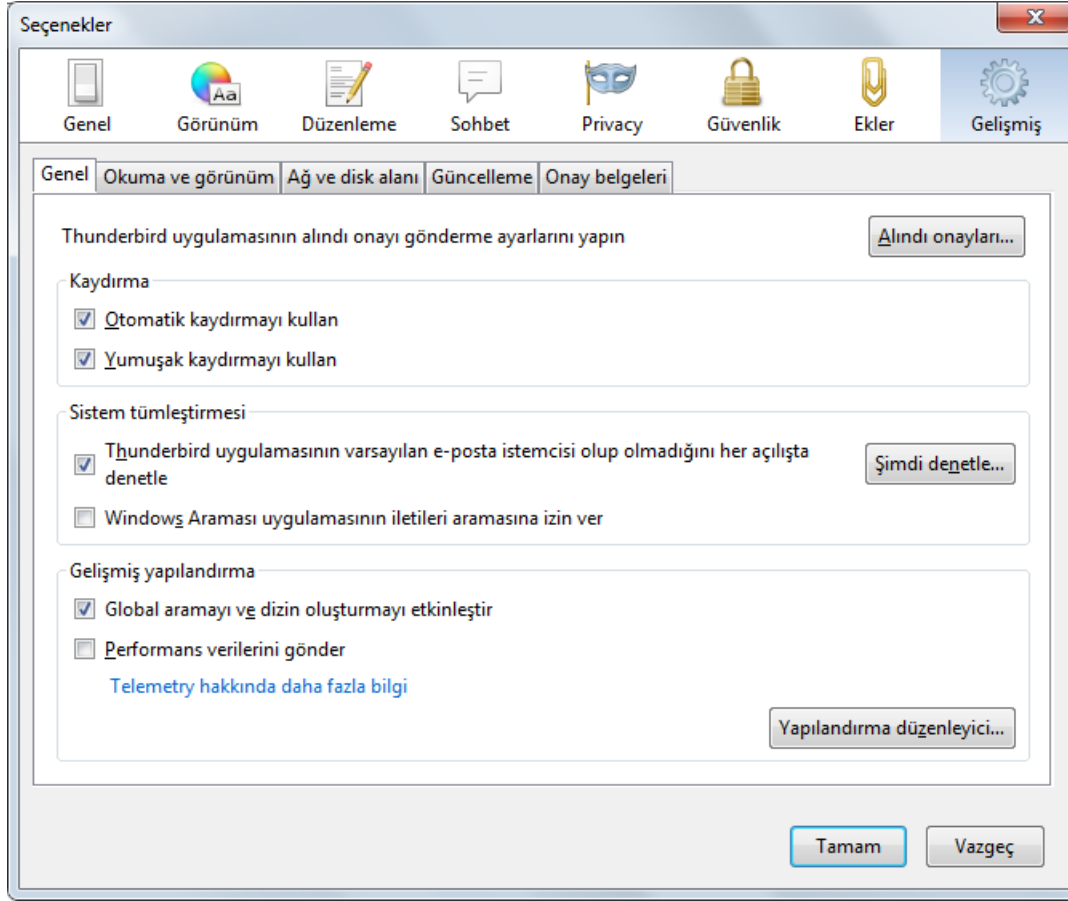
**Uyarı:** Thunderbird'deki Global Arama ve Dizin Oluşturma özelliği programın performansını korumak için kapatılmalıdır. E-postalarınızın miktarına ve büyüklüğüne bağlı olarak, bu özellik, sürekli ve gereksiz bir şekilde sabit sürücünüze bilgi girip ve sisteminizin hızını düşmesine sebep olabilir. Zamanla dolan sabit sürücünüz, pek çok alakasız sistem operasyonlarının çalışmasını da yavaşlatabilir.

Global Arama ve Dizin Oluşturma seçeneğini kapatmak için aşağıdaki adımları uygulayın:

1. Adım. Thunderbird menüsünden Araçlar>Seçenekler'i seçerek Seçenekler ekranını etkinleştirin.

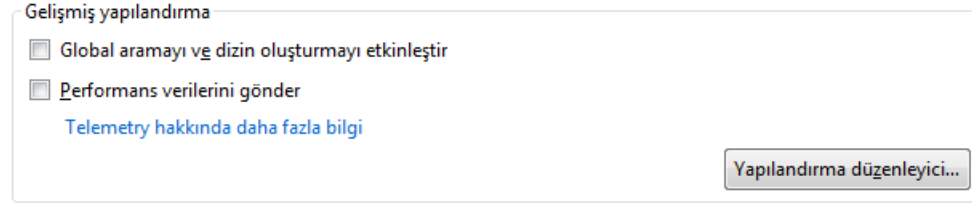


**2. Adım.** Aşağıda görüldüğü gibi gelişmiş seçenekler sekmesini etkinleştirmek için **Gelişmiş** i tıklayın:



Şekil 4: Gelişmiş sekmesi gösterilen Seçenekler ekranı

**3. Adım.** Global arama ve Dizin Oluşturmaya Etkinleştir kutusunu **tıklayarak** bu seçeneği aşağıda görüldüğü gibi **kapatın**:



Şekil 5: Gelişmiş Yapılandırma kısmı

Şimdi bu seçeneği başarı ile kapattığınıza göre **Thunderbird'de** bir e-posta hesabı kaydetmeye hazırsınız.

## 2.2 Thunderbird'de Bir E-Posta Hesabı Nasıl Kaydedilir?

İlk kaydolmada Sistem Tümleştirmesi ekranı belirecek. Bu ekran, 'Thunderbird aşağıdaki hizmetler için varsayılan istemci olarak kullanılsın: E-posta şeklinde ayarlanabilir. Ya da, bu aşamayı atlayabilirsiniz de.

**1. Adım.** Hoşgeldiniz sayfasında *Bunu geç,mevcut e-postamı kullanacağım* seçeneğini **tıklayarak** aşağıdaki ekranı açın:

Thunderbird uygulamasına hoş geldiniz

### Yeni bir e-posta adresi ister misiniz?

İsminiz veya rumuzunuz

Çeşitli sağlayıcılarla ortaklık kuran Thunderbird size yeni bir e-posta hesabı önerebilir. Başlamak için yukarıdaki alana adınızı ve soyadınızı veya istediğiniz diğer kelimeleri yazmanız yeterlidir.

☒  gandi.net

Kullanılan arama terimleri, uygun e-posta adreslerini bulmak için Mozilla'ya (Gizlilik ilkeleri) ve üçüncü parti e-posta sağlayıcılarına [gandi.net (Gizlilik ilkeleri, Hizmet koşulları)] gönderilir.

Şekil 6: Thunderbird Uygulamasına Hoşgeldiniz ekranı

**2. Adım.** İlgili kutucuklara adınızı, e-posta adresinizi ve parolanızı **girin**; *Parolayı Hatırla* kutucuğuna **tıklayarak** işareti kaldırın. Ekranınız Şekil 7'deki gibi görünsün.

Posta Hesabı Kurulumu

İsminiz:  Başkalarına gösterilecek isim

E-posta adresi:

Parola:

☐ Parolayı hatırla

Şekil 7: Posta Hesabı Kurulumu ekranı

**3. Adım.** Aşağıdaki ekranı görmek üzere 'yi **tıklayın**.

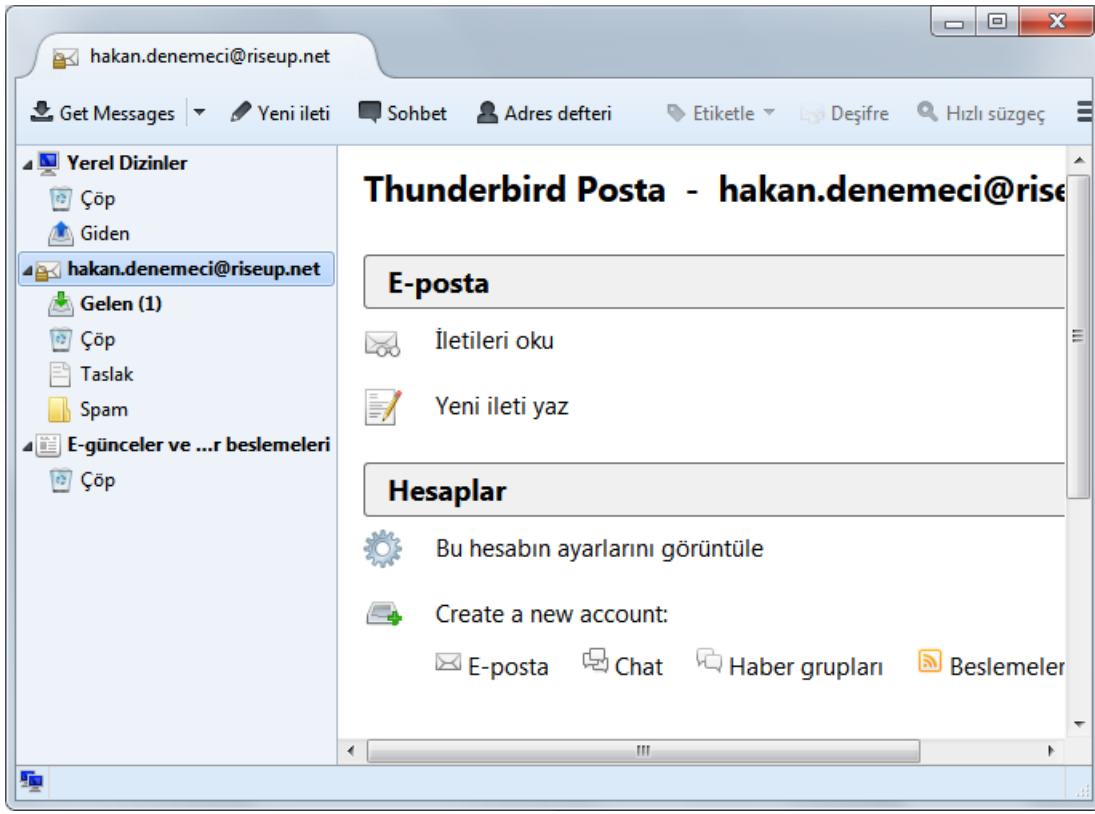
Şekil 8: **IMAP (uzak dizinler)** seçeneği seçilmiş Posta Hesabı Kurulumu ekranı

## IMAP ve POP: Tanımları ve Kullanımları

**Internet Mesajı Ulaşım Protokolü (Internet Message Access Protocol, IMAP)** ve **Ofis Arkası Protokolü (Post Office Protocol, POP)** e-postalarınızı almanın ve saklamanın iki farklı metodudur.

- **Internet Mesajı Ulaşım Protokolü (IMAP):** IMAP kullanılırken bütün dizinleriniz (*gelen, taslak, şablonları, giden* ve bütün diğer dizinler) e-posta sunucusunda kalır. Bu sayede, bu dosyalara başka bilgisayarlardan da ulaşabilirsiniz. İlk aşamada bütün iletiler sunucuda kalırken, sadece e-posta başlıkları ve tanımlayıcı bilgiler (tarih ve zaman, konu, gönderenin adı gibi) bilgisayarınıza indirilerek görünümünüze sunulur. Bir ileti ancak onu açmak istediğinizde bütünüyle bilgisayarınıza indirilir. **Thunderbird** tüm ya da bazı dizinlerdeki e-postaların kopyalarını bilgisayarınıza kaydedecek şekilde de ayarlanabilir, bu sayede bu postalar üstünde çevrimdışı iken de çalışmanız mümkün olur. **IMAP** seçeneği aktif iken bu postaları ya da dizinleri silmek istediğinizde, silme işlemi *hem* lokal olarak kendi bilgisayarınızdan *hem* de sunucudan gerçekleşir.
- **Ofis Arkası Protokolü 3. Versiyonu (POP3):** POP3 kullanıldığında sadece *Gelen* dosyası (yeni gelen postaların bırakıldığı dosya) sunucuda kalır; diğer bütün dosyalar sadece yerel olarak bilgisayarınıza kaydedilir. Gelen postalarınızı okumak için bilgisayarınıza indirdikten sonra, *Gelen* dosyasında bırakabilir ya da sunucudan silebilirsiniz. E-posta hesabınıza başka bir bilgisayardan ulaşmak isterseniz, sadece *Gelen* dosyasındaki mesajları görebilirsiniz (yeni gelen mesajlar ve silmediğiniz eski mesajlar). Dikkat edin, sunucunun ayarlarına bağlı olarak, gönderdiğiniz mesajların kopyaları da sunucuda *Giden* dosyasında korunuyor olabilir. Kontrol etmenizde fayda var.

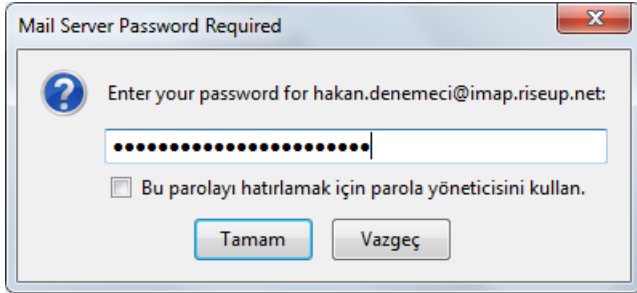
**4. Adım.** Hesabınızı yaratmak için **Bitti** 'ye basın, ve aşağıda görüldüğü gibi solunda e-posta hesabınızı gösteren **Thunderbird** konsolunu açın.



Şekil 9: Yeni yaratılan Riseup hesabını gösteren Mozilla Thunderbird ana kullanıcı arayüzü

**Not:** Başka bir e-posta hesabını eklemek için, **Yerel Dizinler>Hesaplar>Yeni hesap yarat: e-posta'ya tıklayarak** bu bölümde 7. Şekilde görülen ekranı etkinleştirin ve 2., 3. ve 4. adımları tekrarlayın.

E-posta hesaplarınızı **Thunderbird'e** başarıyla kaydettiğiniz takdirde, kullanıcı arayüzünün bir sonraki açılışında her bir kayıtlı e-posta hesabınız için parolanızın tekrar girilmesi aşağıda görüldüğü gibi istenecek:



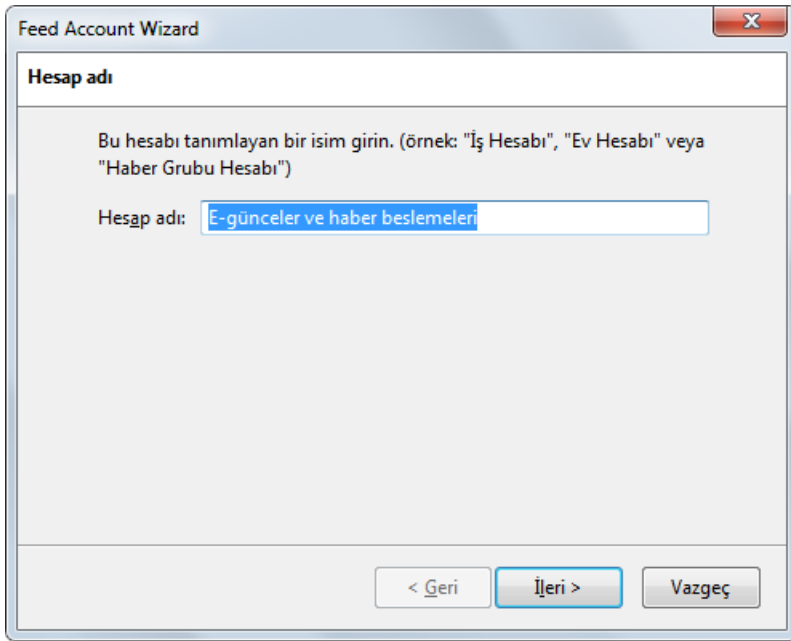
Şekil 10: Posta Sunucusu Parolası Gerekli penceresi

**Not:** İnternet gizliliği ve güvenliği açısından parola kayıt ya da 'hatırlama' fonksiyonlarının kullanımı önerilmese de, **Thunderbird** bir *Ana Parola* fonksiyonuna sahiptir. Bu fonksiyon, kurulum aşamasında girilen tek bir parola ile bütün e-posta hesaplarınıza ilişkin parolaların korunmasını sağlar. Bu özellik hakkında daha fazla bilgi almak için lütfen bölüm **3.3 Thunderbird'de Güvenlik Sekmeleri Nasıl Yapılandırılır?** <sup>[177]</sup> - **Parola Sekmesi**'ne bakın.

## 2.3 Thunderbird'de Bloglar, Haber Akışları ve Haber Grupları Nasıl Kaydedilir?

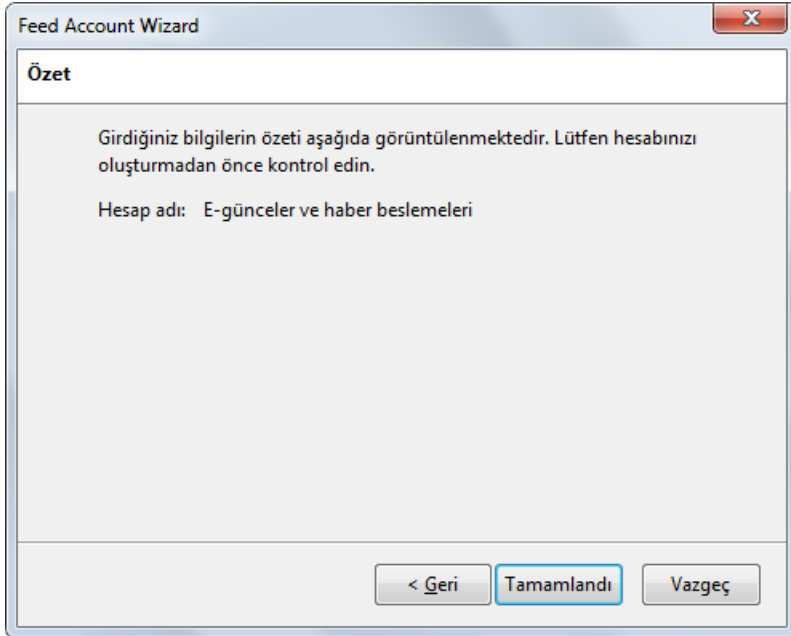
Blogları, haber Akışlarını ve haber gruplarını kaydetmek için aşağıdaki adımları uygulayın:

**1. Adım.** Kenar çubuğundan hesabınızı seçin ve **Hesaplar>Akışlar'a tıklayarak** aşağıda da görülen *Akış Hesabı Sihirbazı* ekranını etkinleştirin.



Şekil 11: Akış Hesabı Sihirbazı – Hesap Adı ekranı

2. Adım. **İleri >** yi tıklayarak aşağıdaki pencereyi etkinleştirin.



Şekil 12: Akış Hesabı Sihirbazı – Tebrikler penceresi

3. Adım. **Son** 'u tıklayıp hesap kurma işlemini tamamlayın ve Thunderbird konsoluna geri dönün.

Şimdi **Thunderbird**'ü optimal kullanım için uygun bir şekilde yapılandırdığınıza göre, lütfen bir sonraki bölüm olan **Thunderbird'de Güvenlik Ayarlarını Yapılandırma**'ya <sup>[178]</sup> geçin.

## Thunderbird'de Güvenlik Ayarlarını Yapılandırma

Bu sayfadaki bölümlerin listesi:

- **3.0 Thunderbird'deki Güvenlik Seçenekleri Hakkında**
- **3.1 Thunderbird'de Önizleme Bölmesi Nasıl Kapatılır?**
- **3.2 Thunderbird'de HTML Özelliği Nasıl Kapatılır?**
- **3.3 Thunderbird'de Güvenlik Sekmeleri Nasıl Yapılandırılır?**
- **3.4 Hesap Ayarları Gereksiz Posta Filtresi Nasıl Açılır?**

### 3.0 Thunderbird'deki Güvenlik Seçenekleri Hakkında

**Mozilla Thunderbird** bağlamında güvenlik, genel olarak bilgisayarınızın zararlı ya da kötü niyetli e-posta iletilerine karşı

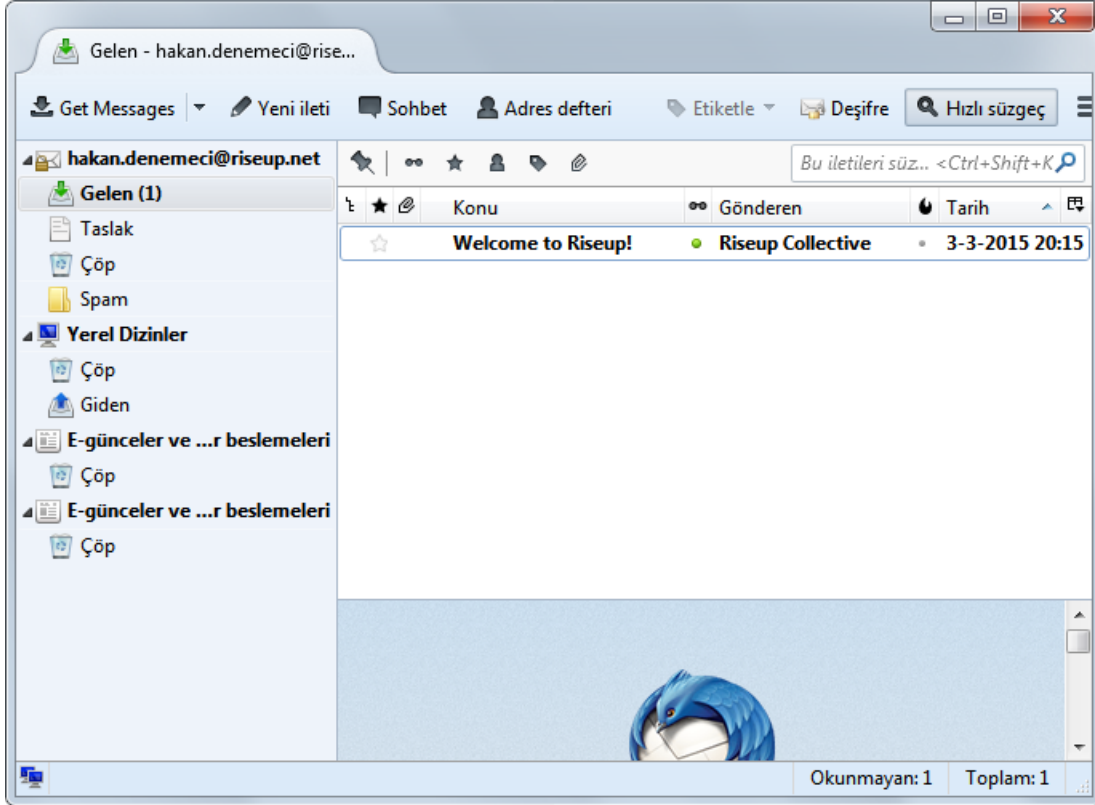
korumak anlamına gelir. Bunlardan bazıları sadece reklam olabilir, diğerleri casus yazılımlar ya da virüsler içerebilir. **Mozilla Thunderbird**'ün sisteminizi e-postalardan kaynaklanan saldırılardan koruyabilme yetisi güçlendirmek için yapılandırılması, açılması ya da kapatılması gereken birkaç ayar var. Bunun ötesinde, kötü amaçlı yazılım karşıtı ve güvenlik duvarı yazılımlarının da bilgisayarınızda kurulu olması **çok önemlidir**.

Zararlı ya da kötü niyetli yazılımları durdurmaya yönelik ve, **Avast** <sup>[179]</sup>, **Comodo Firewall** <sup>[180]</sup> ve **Spybot** <sup>[181]</sup> gibi yazılımlar hakkında bilgi almak için lütfen şuraya bakınız: Nasıl Yapmalı Kitapçığı **1. Bölüm Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz** <sup>[182]</sup>

### 3.1 Thunderbird'de Önizleme Bölmesi Nasıl Kapatılır?

**Thunderbird** ana penceresi üç bölgeye ayrılır: soldaki kenar çubuğu e-posta hesaplarınızın dizinlerini, sağ taraf ileti listesini ve alt bölme seçilen bir e-posta iletinizin *önizlenimini* gösterir. Bu önizlenim bir ileti üstüne tıklanır tıklanmaz otomatik olarak açılır.

**Not:** Bir e-posta kötü niyetli bir kod içeriyorsa, *önizlenim* bölümü bu kodu etkinleştirebilir; bu yüzden önizlemeyi kaldırmak iyi bir fikirdir.



Şekil 1: Thunderbird ana kullanıcı arayüzü

Önizlenim bölümünü kaldırmak için aşağıdaki adımı uygulayın:

**1. Adım.** 'ü tıklayarak **Thunderbird Menü'sünü** görün ve **Seçenekler>Yerleşim>İleti Bölmesi F8'i** aşağıdaki gibi seçin:

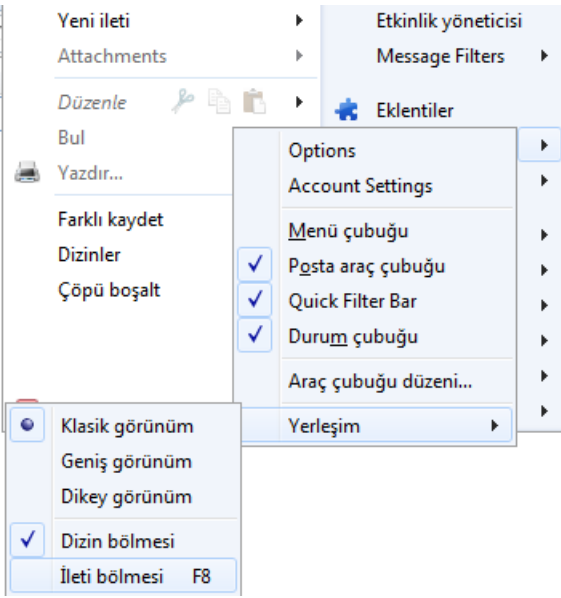


Figure 2: Düzen alt menüsü ve seçimi kaldırmış İleti Bölmesi opsiyonu açık görülen Seçenekler menüsü

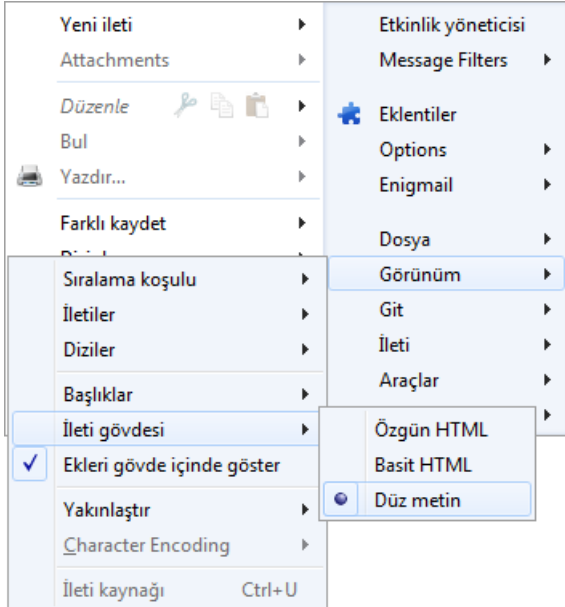
**İleti bölmesi** kaybolacak. Bundan böyle bir e-posta iletisinin içeriğini görebilmek için ona **çift tıklamanız** gerekli olacak. Artık, şüpheli görünen bir e-posta gördüğünüzde (belki beklenmedik ya da ilgisiz bir konu başlığı varsa, ya da tanınmayan biri tarafından yollanmışsa) e-postayı içeriğini görmeden silmeyi seçebilirsiniz.

## 3.2 Thunderbird'de HTML Özelliği Nasıl Kapatılır?

**Thunderbird** iletileri yazma ve okuyabilmeniz için **Zengin Metin İşaret Dili (HyperText Markup Language, HTML)** kullanır. Bu renk, font, şekil ve diğer biçimlendirme özelliklerini kapsayan iletiler alıp göndermenizi sağlar. Fakat **HTML** aynı zamanda Web sayfaları için kullanılan bir dildir, iletileri **HTML** biçimlendirmesiyle görüntülemek sizi internet sayfalarının oluşturabileceğine benzer tehditleri barındıran kötü niyetli e-postaların etkilerine açık bırakabilir.

**HTML** biçimlendirmesi özelliğini kapatmak için aşağıdaki adımı uygulayın.

**1. Adım.** 'ü tıklayarak **Thunderbird Menüsünü** açın ve aşağıda görüldüğü gibi **Seçenekler>Görünüm>İleti Gövdesi>Düz Metin**'i seçin:



Şekil 3: İleti Metni altmenüsünde Düz Metin seçeneği seçilmiş Görünüm menüsü

## 3.3 Thunderbird'de Güvenlik Sekmeleri Nasıl Yapılandırılır?

**Thunderbird**'ün iki yerleşik gereksiz posta filtresi size hangi postaların gereksiz posta olduğuna karar vermenizde yardımcı olur, ve bunların kullanılabilmesi için önce etkinleştirilmeleri gereklidir. Bu filtreler etkinleştirildikten sonra gereksiz postaları almaya devam edeceksiniz, ama bunlar **Thunderbird** tarafından otomatik olarak **Gereksiz** dizinine yönlendirilecek.

Aynı zamanda **e-dolandırıcık** denilen e-postalarla yapılan sahtekarlıklar, genelde sizi e-posta içindeki bir linki tıklamanızı

sağlamaya çalışır. Bu linkler çoğunlukla internet tarayacınızı bilgisayarınıza bir virus bulaştırmaya çalışarak bir web sitesine yönlendirir. Diğer durumlarda link sizi geçerli bir kullanıcı adı ve şifre girmeye ikna edebilecek kadar meşru görünen bir siteye yönlendirir. Bu verilen kullanıcı adları ve şifreler daha sonra kullanılmak ya da ticari ve de kötü niyetli amaçları olan üçüncü partilere satılmak için saklanır.

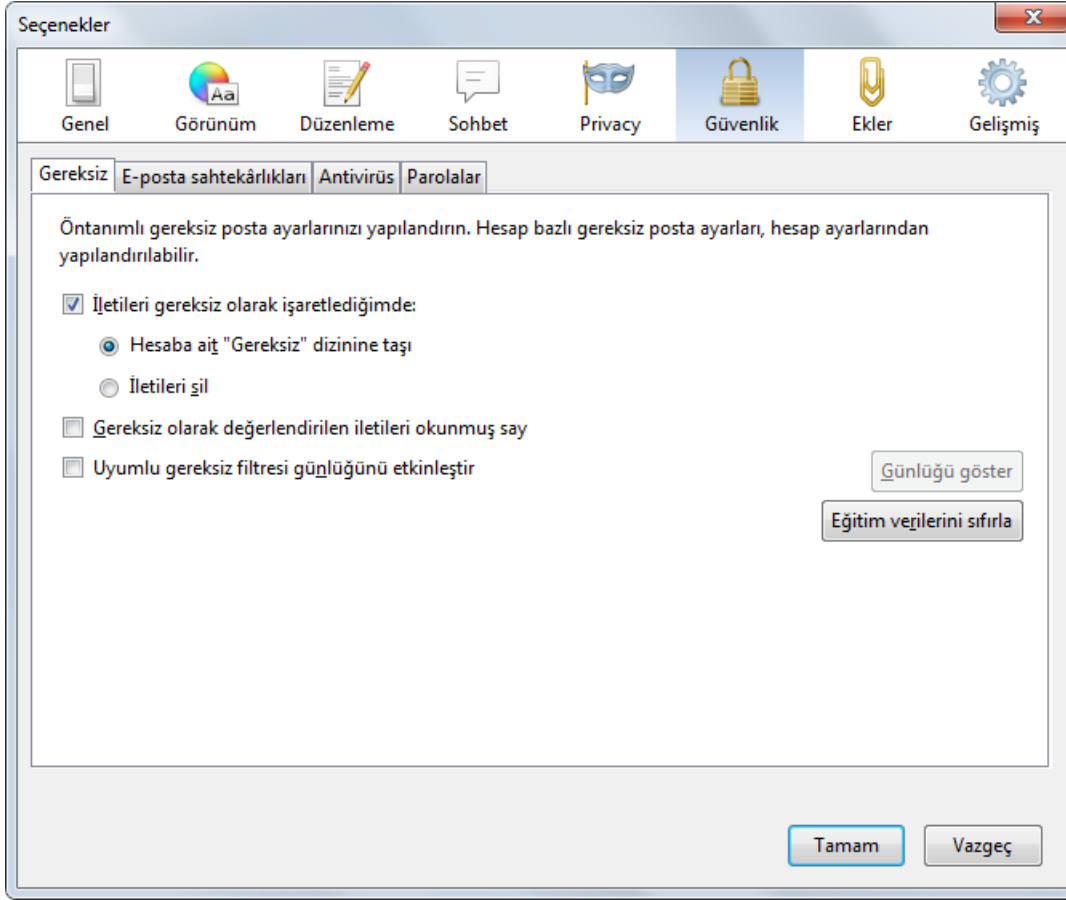
**Thunderbird** bunun gibi e-postaları tespit etmenize yardımcı olup sizi uyarma kapasitesine sahiptir. Kötü niyetli web sitelerinden kaynaklanan saldırılara karşı diğer korunma araçları **Firefox** bölümünün **Diğer Kullanışlı Mozilla Eklentileri** [183] kısmında tarif edilmiştir.

Gereksiz posta ve güvenlik kontrolleri farklı yerlerde konumlandırılmıştır. Bunların bir kısmına *Seçenekler - Güvenlik* penceresinden ulaşabilirsiniz. Buradaki kontroller aracılığıyla gizlilik ve güvenlik seçeneklerinin büyük bir kısmı yapılandırılabilir. Bu kontrollere ulaşmak için aşağıdaki adımları takip edin:

**1. Adım. Menü > Seçenekler'i seçerek Seçenekler** penceresini etkinleştirin.



**2. Adım.** 'Güvenlik' i tıklayarak aşağıdaki ekranı etkinleştirin:



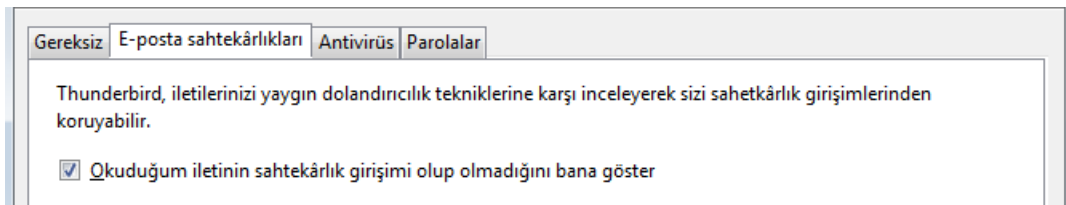
Şekil 4: İlgili sekmeleri görünen Güvenlik penceresi

## Gereksiz Posta sekmesi

**1. Adım. Thunderbird'ün** sizin gereksiz posta olarak belirlediğiniz postaları silmesi için *Şekil 4*'te gösterildiği gibi *Gereksiz* sekmesindeki ilgili seçenekleri **işaretleyin**.

## E-Posta Sahtekarlığı sekmesi

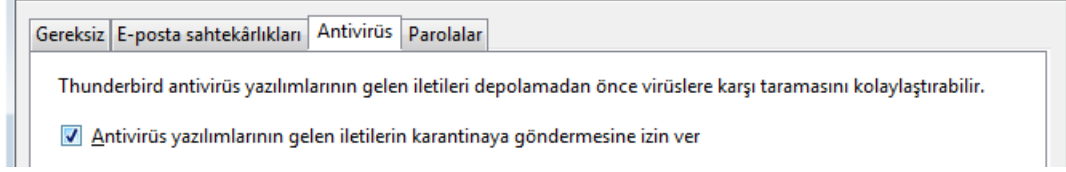
**1. Adım. Thunderbird'ün** iletilerinizi e-posta sahtekarlığı için analiz etmesi için 'Okuduğum ileti şüpheli bir e-posta sahtekarlığıysa beni uyar'ı aşağıda görüldüğü gibi **işaretleyin**.



5. Şekil: E-Posta Sahtekarlığı sekmesi

## The Anti-Virus tab

1. Adım. Aşağıdaki ekranı etkinleştirmek için *Antivirüs* sekmesini **tıklayın**:



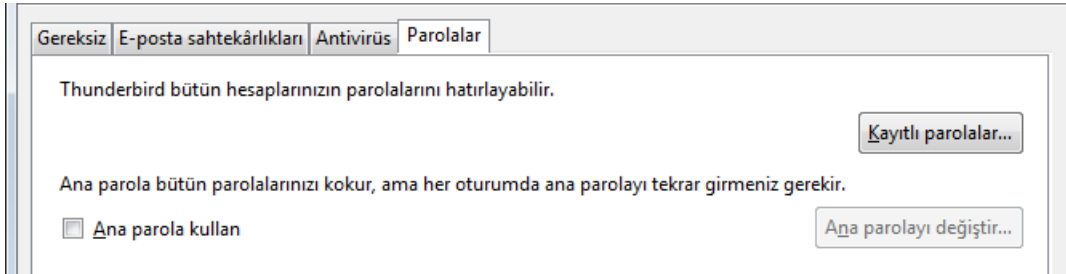
Şekil 6: Antivirüs sekmesi

Bu seçenek iletilerinizin antivirus yazılımınız tarafından taranıp ayrıştırılmasını sağlar. Bu ayar etkin olmazsa, virüslü bir ileti aldığınızda *bütün gelen* kutunuzun *karantinaya* alınması mümkündür.

**Not:** Bu adım çalışan bir antivirus programınız olduğunu varsayar. Antivirüs programını nasıl kurup yapılandırabileceğinize dair bilgi almak için lütfen **Avast** <sup>[184]</sup>'a bakın.

## Parolalar Sekmesi

1. Adım. *Parolalar* sekmesini **tıklayarak** aşağıdaki ekranı **etkinleştirin**:

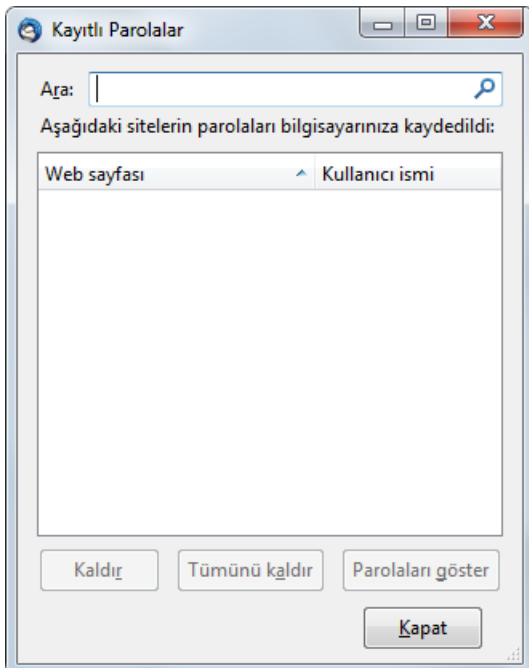


Şekil 7: Parolalar sekmesi

**Dikkat:** Parolalarınızı gizli tutmanız ve onların güvenliğini sağlamanız için tasarlanmış olan bir program kullanmanızı şiddetle tavsiye ederiz; daha fazla bilgi edinmek için lütfen **KeePass** <sup>[13]</sup>'e başvurun.

**Not:** *Parolalar* sekmesindeki seçenekler, e-posta hesaplarınızı **Thunderbird'de** ilk kaydettiğiniz esnada, *Posta Hesabı Kurulumu* ekranında *Parolaları Hatırla* seçeneğini işaretlediyseniz etkin olacaktır.

1. Adım. **Kayıtlı parolalar...** <sup>[1]</sup> tıklayarak aşağıdaki ekranı etkinleştirin:

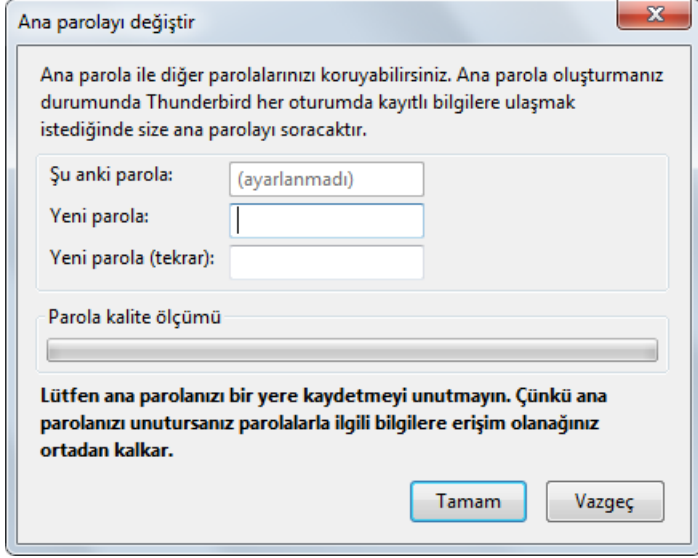


Şekil 8: Kayıtlı Parolalar penceresi

*Kayıtlı Parolalar* penceresi bütün hesaplarınızla ilişkili parolalarınızı kaldırmanızı ya da görüntülemenizi sağlar. Yine de, gizliliğinizi ve güvenliğinizi daha da yükseltmek için, bütün e-posta hesaplarınıza erişimi bir *Ana Parola* belirleyerek

koruyabilirsiniz. Bu **Thunderbird**'ün parola seçenekleri ile tanıdık olan bir kimsenin sizin hesap parolalarınıza ulaşımını engeller.

**3. Adım.** Ana parola kullan seçeneğini Şekil 7'de görüldüğü gibi **işaretiliyerek** aşağıdaki ekranı etkinleştirin.

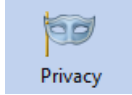


Şekil 9: Ana Parolayı Değiştir penceresi

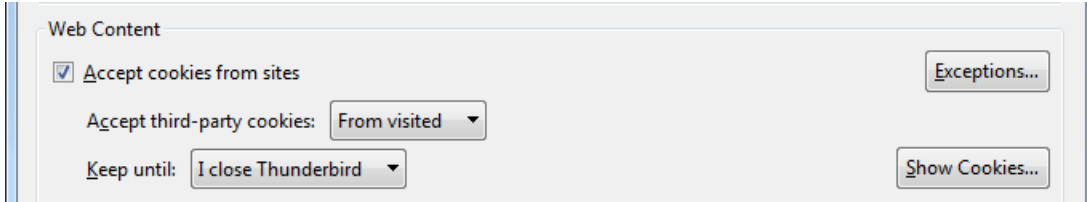
**5. Adım.** Yeterince güçlü olan ve sadece sizin hatırlayabileceğiniz bir parola **girin** ve **Tamam** butonunu **tıklayarak** bunu teyit edin.

## Web İçeriği

Web tarayıcınızın bir web sitesinin kimliğini denetlemek ya da tespit etmek için kullandığı kısa metinlere çerez denir. *Web İçeriği* seçeneği hangi blog, haber akışı ya da haber grubuna ait çerezlerin güvenilir ve emniyetli olduğunu belirlemenizi sağlar.



**1. Adım.** **Privacy** butonuna tıklayarak Web İçeriği seçeneklerini aşağıda görüldüğü gibi açın:



Şekil 10: Gizlilik Sekmesi

**2. Adım.** Şu ana kadar sakla altında Ben Thunderbird'ü kapatana kadar'ı seçin: bu seçenek çerezleri **Thunderbird**'ü her kapatışınızda çerezleri silerek güvenliğinizi artırır.

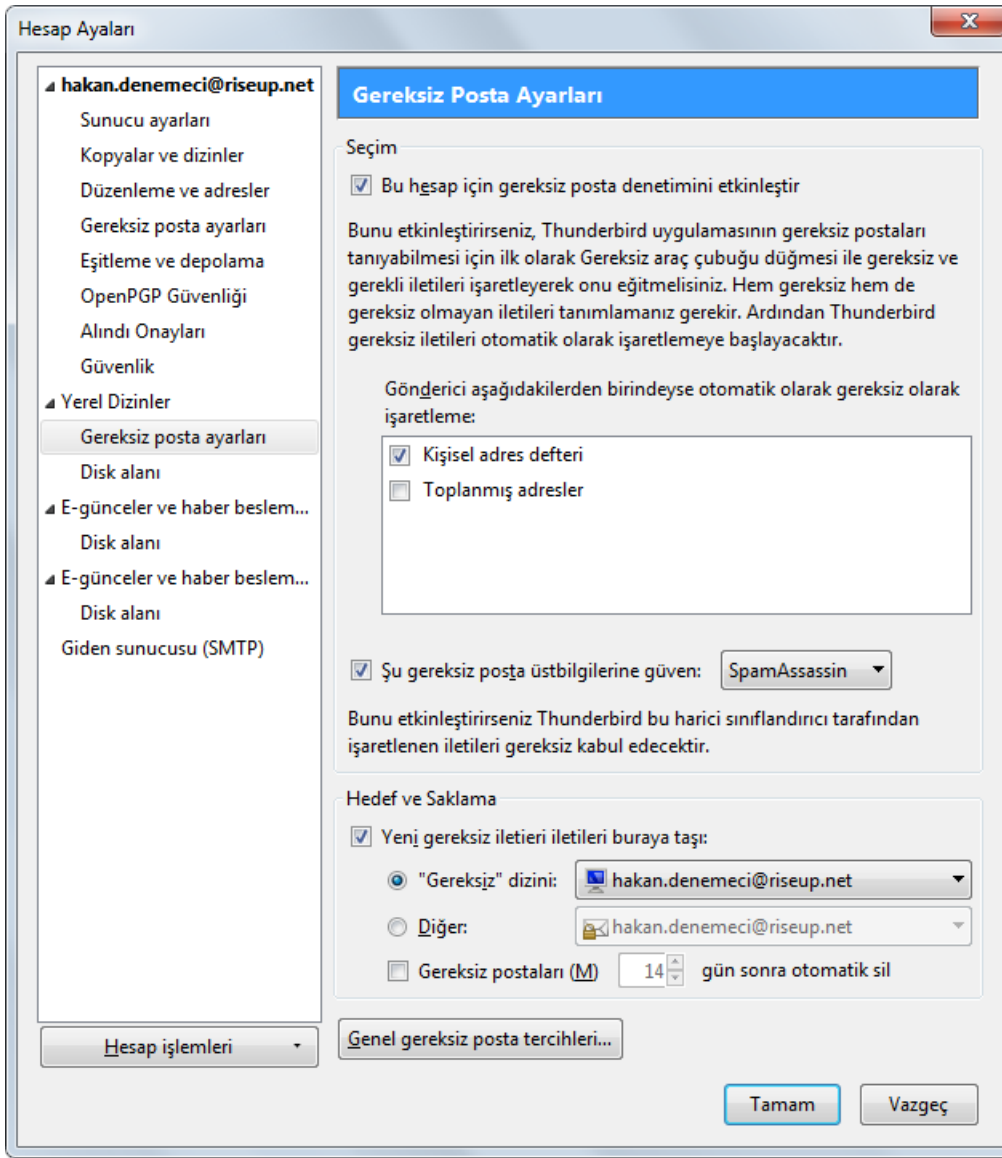
## 3.4 Hesap Ayarları - Gereksiz Posta Filtresi Nasıl Açılır?

İkinci tür **Thunderbird** gereksiz posta filtresine Hesap Ayarları – Gereksiz Posta Ayarları penceresinden ulaşılabilir. Bu filtreler verili olarak etkin değildir, bu yüzden bunları kullanmak isterseniz etkinleştirmeniz gerekir. Böylelikle gereksiz posta teslim alındığında **Thunderbird** onu otomatik olarak değişik hesaplarla ilgili Gereksiz dizinlerine yönlendirir.

**1. Adım.** Seçenekler > Hesap Ayarları'nı seçerek Hesap Ayarları penceresini etkinleştirin.

**2. Adım.** Kenar çubuğunda görülen belirli bir **Gmail** ya da **RiseUp** hesabıyla ilişkili Gereksiz Posta Ayarları seçeneğini seçin.

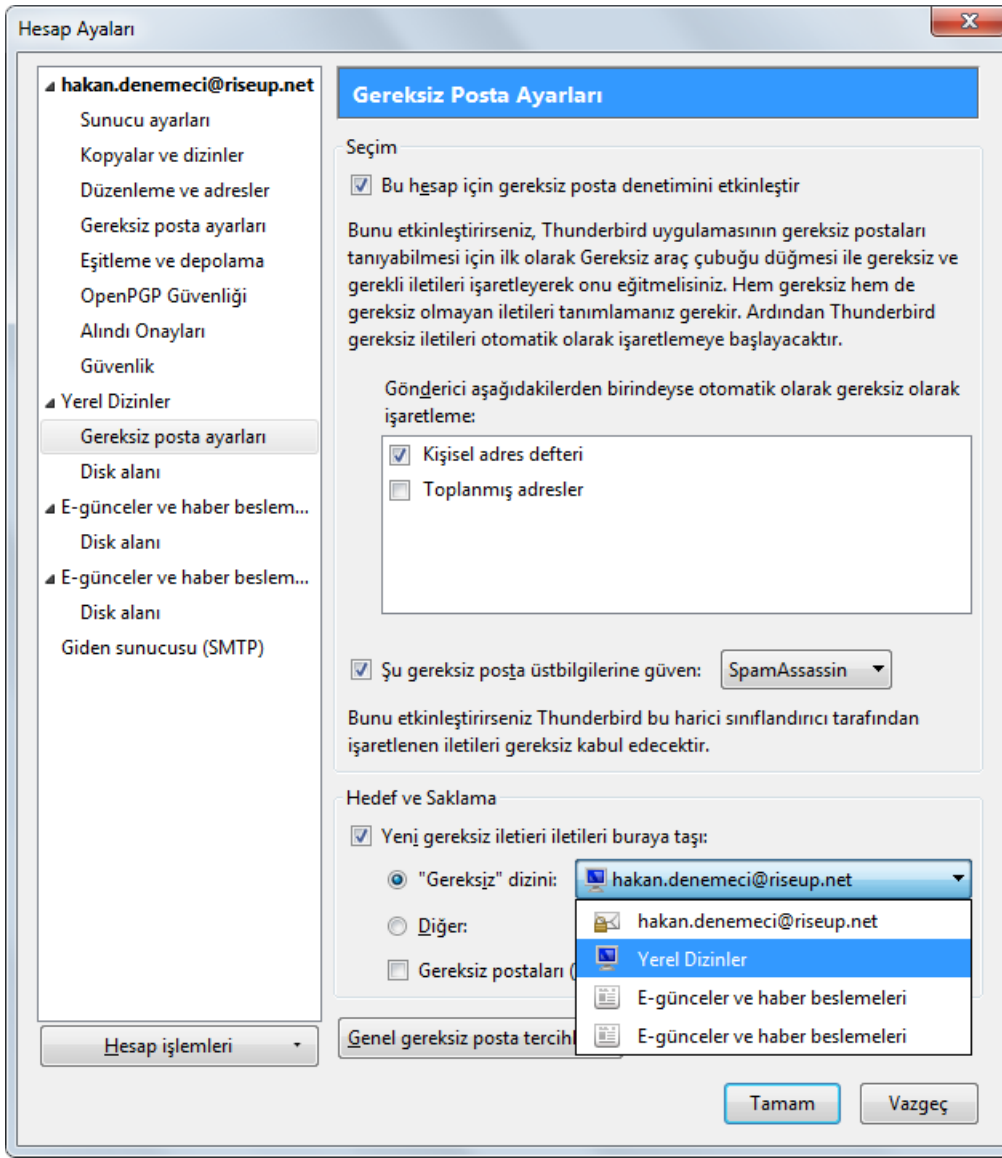
**3. Adım.** Gereksiz Posta Ayarlarını **etkinleştirin** ve Hesap Ayarları- Gereksiz Posta Ayarları ekranı aşağıdakine benzesin:



Şekil 11: Hesap Ayarları – Gereksiz Posta Ayarları penceresi

4. Adım: **Tamam** butonunu tıklayarak Hesap Ayarları penceresinin yapılandırılmasını tamamlayın.

**Not:** Gereksiz Posta Ayarları her bir hesap için ayrı ayrı yapılandırılmalıdır. Böylelikle, bir **Gmail** ya da **RiseUp** hesabına gelen **Gereksiz Postalar** ilgili **Çöp** dosyasına yerleştirilecektir. Bunun yerine bütün hesaplarınızın gereksiz postalarını sizin belirlediğiniz bir **Yerel Dizin**e yönlendirebilirsiniz.



Şekil 12: Hesap Ayarları - Gereksiz Posta Ayarları penceresi, merkezi bir gereksiz posta dizini için ayarları gösteriyor

1. Adım: Gereksiz Posta Ayarları'nı **Seçin**, bu, kenar çubuğunda *Yerel Dizinler*'in hemen altındadır.
2. Adım: Gereksiz Postaları Yönlendir aşağı açılır listesinden *Yerel Dizinler*'i Şekil 12'de görüldüğü gibi **seçin**.
3. Adım. **Tamam** butonunu tıklayarak Hesap Ayarları penceresinin yapılandırılmasını tamamlayın.

Şimdi **Thunderbird'deki** farklı güvenlik seçenekleri ve gereksiz posta ayarlarını yapılandırıdığınıza göre, lütfen bir sonraki **Thunderbird'de GnuPG'li Enigmail Nasıl Kullanılır?** <sup>[185]</sup> bölümüne devam edebilirsiniz.

## Thunderbird'de GnuPG ile Enigmail Nasıl Kullanılır?

Bu sayfadaki kısımların listesi:

- **4.0 Enigmail, GnuPG ve Açık-Kişisel Anahtar Şifreleme ile İlgili Genel Bilgiler**
- **4.1 Enigmail ve GnuPG Nasıl Yüklenir?**
- **4.2 Anahtar Çiftleri Nasıl Oluşturulur ve Enigmail Kendi E-posta Hesaplarınızla Uyumlu Çalışacak Şekilde Nasıl Yapılandırılır?**
- **4.3 Açık Anahtarlar Nasıl Paylaşılır?**
- **4.4 Anahtar Çifti Nasıl Doğrulandır ve İmzalanır?**
- **4.5 Bir Mesaj Nasıl Şifrelenir ve Bir Mesajın Şifresi Nasıl Çözülür?**

### 4.0 Enigmail, GnuPG ve Açık-Kişisel Anahtar Şifreleme ile İlgili Genel Bilgiler

**Enigmail** e-posta iletişim gizliliğinizi korumaya yarayan bir **Mozilla Thunderbird** eklentisidir. **Enigmail GnuPG** şifreleme programını **Thunderbird**'ün içinde kullanmanıza izin veren bir arayüzdür. **Enigmail** arayüzü, **Thunderbird** konsol araç çubuğunda **Enigmail** olarak görülür

**Enigmail açık-anahtarlı şifreyazımına** <sup>[186]</sup> dayanır. Bu yöntemle kişi kendi kişisel anahtar çiftini oluşturmaktadır. Oluşturulan ilk anahtara *kişisel* anahtar denir. Kişisel anahtar bir kullanıcı şifresi veya parola tarafından korunur ve *asla kimse* ile paylaşılmaz.

İkinci anahtara *açık anahtar* denir. Bu anahtar iletişim kurduğunuz kimseler ile paylaşılabilir. Ancak herhangi bir kişinin *açık anahtarını* edindikten sonra bu kişiye şifrelenmiş e-posta gönderebilirsiniz. Bu kişi eşleşen *kişisel anahtara* erişimi olan tek kişi olduğu için, e-postanızın şifresini çözeabilen ve onu okuyabilen tek kişi de odur.

Aynı şekilde, kendi *açık şifrenizin* bir kopyasını e-posta iletişimde olduğunuz insanlara gönderir ve eşleşen *kişisel anahtarı* gizli tutarsanız, bu kişilerden gelecek şifreli mesajları yalnızca siz okuyabilirsiniz.

**Enigmail** aynı zamanda mesajlarınıza *dijital imza* eklemenize de olanak verir. *Açık şifrenize* sahip olan kişi, e-postanın sizden geldiğini bu şekilde doğrulayabilir ve içeriğinin bir başkası tarafından değiştirilmediğinden emin olabilir. Benzer bir biçimde, iletişimde olduğunuz kişinin *açık anahtarına* sahipseniz, onun imzalanmış mesajlarındaki dijital imzasını doğrulayabilirsiniz.

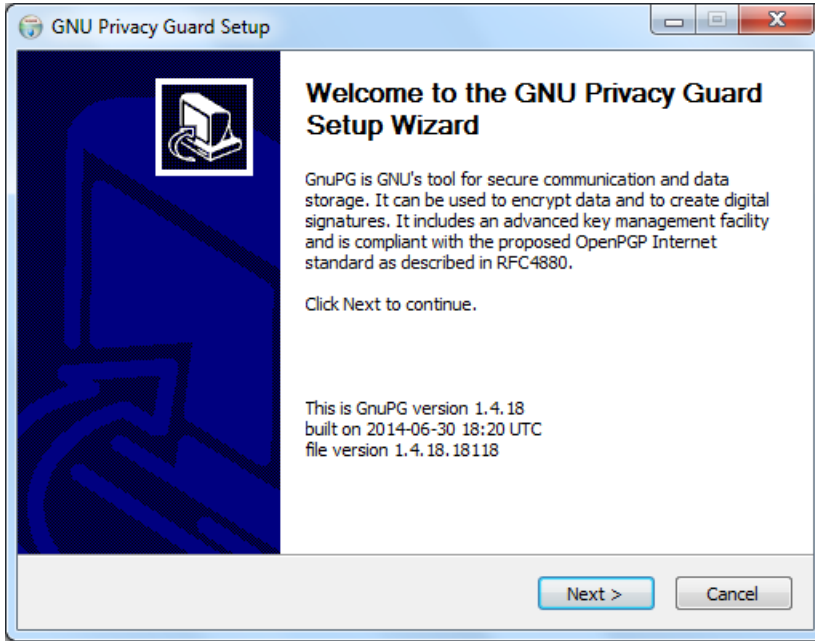
## 4.1 Enigmail ve GnuPG Nasıl Yüklenir?

**Enigmail** ve **GnuPG**'nin nasıl indirileceği konusunda bilgi almak için lütfen [indirme kısmına](#) <sup>[55]</sup> bakın.

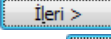
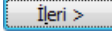
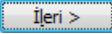
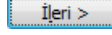
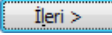
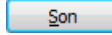
### 4.1.1 GnuPG nasıl kurulum?

**GnuPG**'yi kurmak oldukça basittir. Daha önce yaptığınız yazılım kurma işlemlerinden farklı değildir ve aşağıdaki adımları izleyerek gerçekleştirilebilir:

**1. Adım.** Kurulum işlemini başlatmak için  **gnupg-w32cli-1.4.18.exe** 'ye **çift tıklayın**. *Dosyayı Aç – Güvenlik Uyarısı* iletişim kutusu ekranda belirirse **Çalıştır** 'ı) (Çalıştır) **tıklayın**, aşağıdaki ekran belirecek:



Şekil 1: GNU Gizlilik Koruma Kurulum Sihirbazı

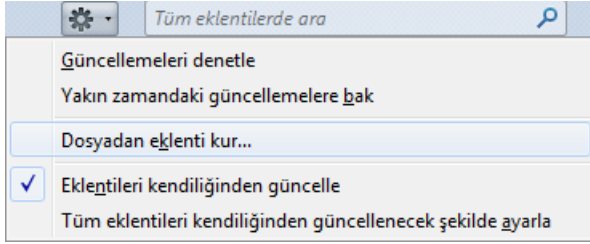
- 2. Adım.** **GNU Gizlilik Koruma Kurulumu – Lisans Anlaşması** penceresini etkinleştirmek için  'yi tıklayın. Okuduktan sonra **GNU Gizlilik Koruma Kurulumu – Bileşen Seçimi** penceresini etkinleştirmek için  'yi **tıklayın**.
- 3. Adım.** Varsayılan ayarları kabul etmek ve **GNU Gizlilik Koruma Kurulumu – Kurulum Seçenekleri – GnuPG Dil Seçimi** penceresini etkinleştirmek için  'yi **tıklayın**.
- 4. Adım.** Aşağı açılır menüden *Türkçe*'yi seçin ve **Kurulum Yerini Seç** penceresini etkinleştirmek için  'yi **tıklayın**.
- 5. Adım.** Varsayılan kurulum yolunu kabul etmek ve **Başlangıç Menüsü Dosyası Seç** ekranını etkinleştirmek için  'u **tıklayın**.
- 6. Adım.** Paket açmayı ve çeşitli **GnuPG99** paketlerini kurmayı başlatmak için  'u **tıklayın**. Bu işlem tamamlandıktan sonra, **Kurulum Tamamlandı** ekranı görünecek.
- 7. Adım.** **GnuPG** programı kurulumunu tamamlamak için  ve daha sonra  'u **tıklayın**.

### 4.1.2 Enigmail Eklentisi Nasıl Kurulur?

**GnuPG** yazılımının kurulumunu başarı ile gerçekleştirdikten sonra **Enigmail** eklentisini kurmaya hazırsınız.

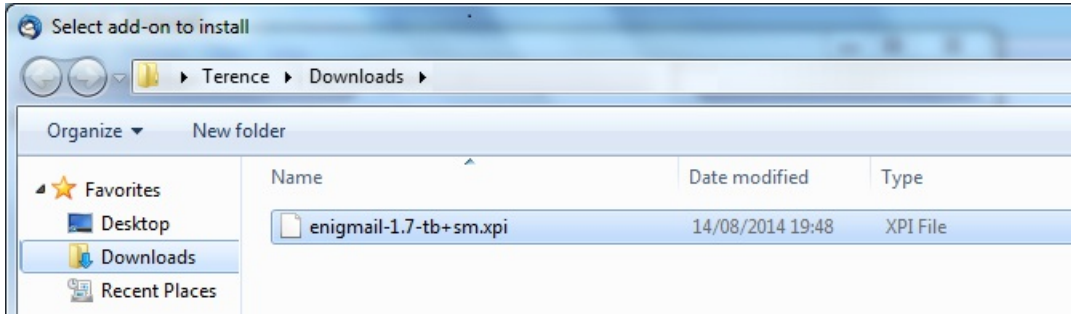
**Enigmail** kurulumu için aşağıdaki adımları takip edin:

- 1. Adım.** **Thunderbird'ü açın** ve 'i **tıklayın**. Açılan *Thunderbird Menü'sünden Eklentileri seçin* ve *Eklenti Yöneticisi* penceresini etkinleştirin.
- 2. Adım.** Sol taraftaki kenar çubuğunda 'i **tıklayın**. Enigmail Eklenti'si henüz bulunamadıysa, *Kurulmuş Bu Tip Eklentiniz Bulunmamaktadır* mesajını göreceksiniz.
- 3. Adım.** Enigmail Eklentisi *Uzantı* panelinde görünürse 'u **tıklayın**. Eğer görünmezse 'i **tıklayın** ve aşağıda görüldüğü şekilde *Eklenti Dosyadan Kur'u seçin*:

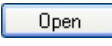


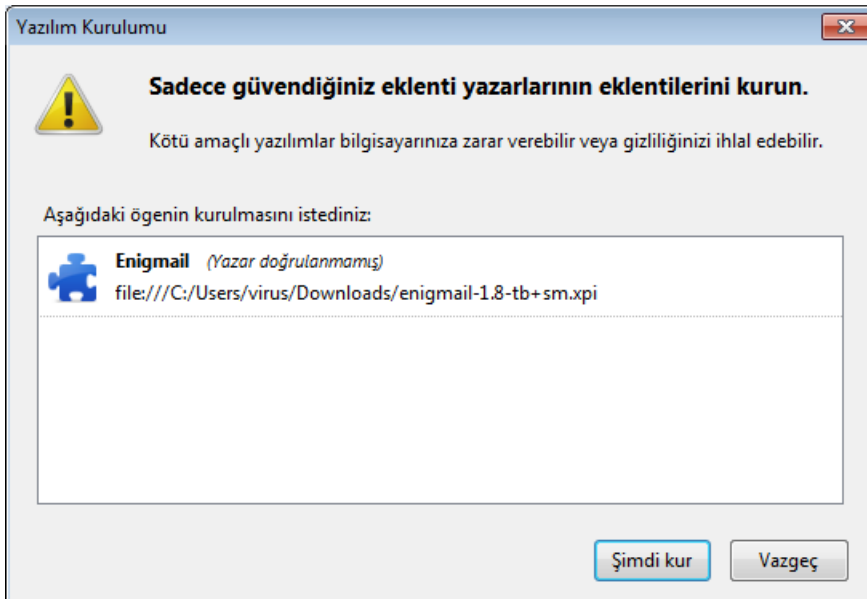
Şekil 3: Eklentiler için Araçlar Menüsü

- 4. Adım.** Aşağıda görüldüğü gibi Enigmail uzantısını kaydettiğiniz klasöre gidin (büyük ihtimalle *İndirilenler* klasörü):



Şekil 4: Kurulacak bir Uzantı Seçin

- 5. Adım.** Aşağıdaki ekranı etkinleştirmek için 'ı **tıklayın**:

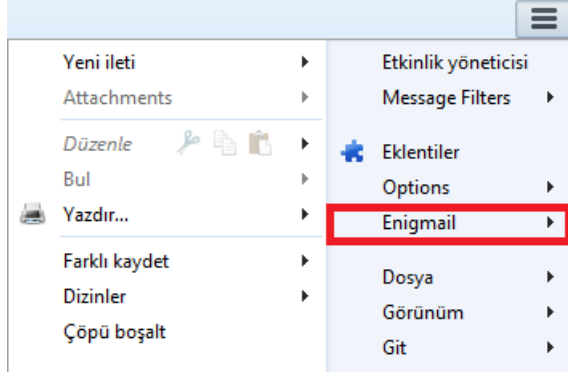


Şekil 5: Yazılım Kurulumu Penceresi

**Önemli:** 6. Adım'ı uygulamadan önce yaptığınız tüm çevrimiçi işlemleri kaydettiğinizden emin olun!

6. Adım. **Şimdi kur** u **tıklayın** ve daha onra **Enigmail** eklentisi kurulumunu tamamlamak için **Şimdi yeniden başlat (R)** ı **tıklayın**.

**Enigmail** eklentisi kurulumunun başarı ile gerçekleştiğinden emin olmak için **Thunderbird** ana kullanıcı arayüzüne geri dönün ve **☰** i **tıklayın**. *Enigmail'in* aşağıdaki gibi seçenekler arasında yer aldığından emin olun.

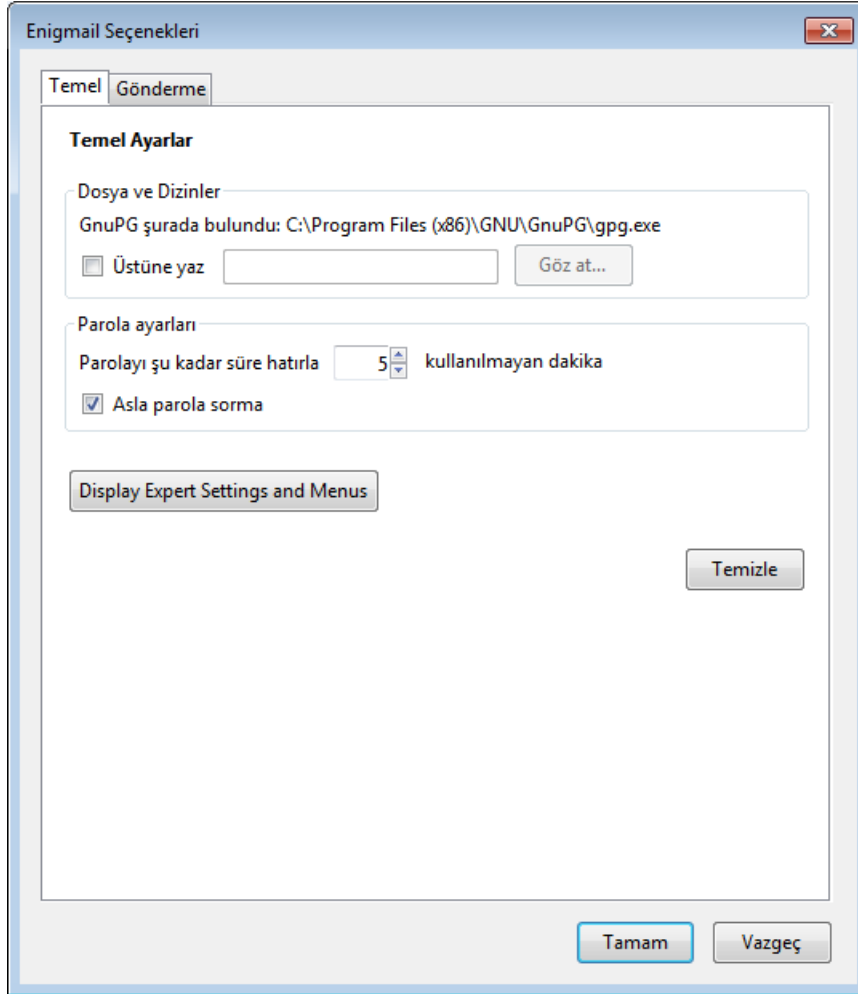


Şekil 6: Thunderbird araç çubuğu ve işaretlenmiş olan Enigmail

### 4.1.3 Enigmail ve GnuPG'nin Çalıştığından Nasıl Emin Olunur?

E-postalarınızın kimlik doğrulamasını yapmak ve onları şifrelemek için **Enigmail** ve **GnuPG** kullanmaya başlamadan önce, bu iki yazılımın birbiri ile iletişim içinde çalıştığından emin olmalısınız.

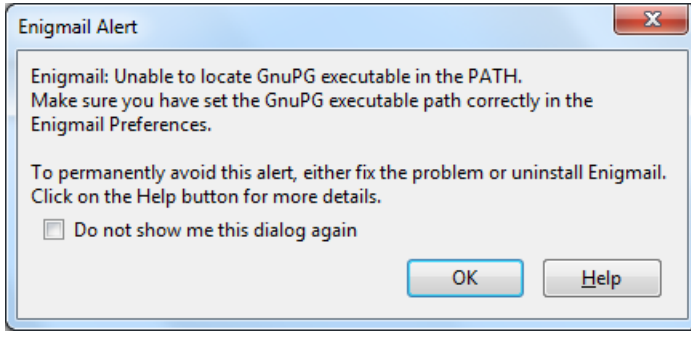
1. Adım. **Enigmail > Tercihleri'i seçin** ve aşağıda görüldüğü gibi *Enigmail Tercihler* ekranına ulaşın:



Şekil 7: Enigmail Tercihler penceresi

**GnuPG** başarılı bir şekilde kurulmuşsa *Dosyalar ve Dizinler* bölümünde şunu göreceksiniz:

GnuPG şurada bulundu: C:\Program Files (x86)\GNU\GnuPG\gpg.exe . Aksi takdirde, aşağıdakine benzer bir uyarı ile karşılaşabilirsiniz:



Şekil 8: Enigmail Uyarı Açılır Mesajı

**İpucu:** Bu mesajı alıyorsanız **GnuPG'yi** kurmadınız veya başka bir yere kurdunuz demektir. **GnuPG'yi** başka bir yere kurduysanız, **Tara...** tuşunu etkinleştirmek seçeneği için **Üstüne Yaz'ı** işaretleyin. Daha sonra **GnuPG programını bul'u** etkinleştirmek için **Browse...** 'ı **tıklayın** ve bilgisayarınızda **gpg.exe** dosyasının olduğu yere gidin. Bu işlem başarılı olmuyorsa, lütfen **4.1 Enigmail ve GnuPG Nasıl Kurulur?** Bölümüne geri dönün.

**2. Adım.** Thunderbird konsoluna geri dönmek için **Tamam** 'ı **tıklayın**.

## 4.2 Anahtar Çiftleri Nasıl Oluşturulur ve Enigmail Kendi E-posta Hesaplarınızla Uyumlu Çalışacak Şekilde Nasıl Yapılandırılır?

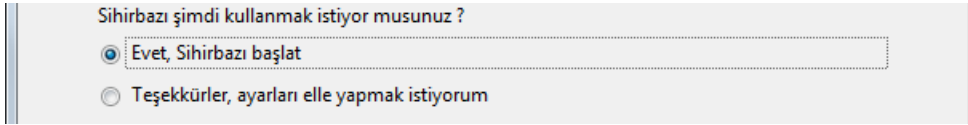
**Enigmail** ve **GnuPG'nin** düzgün bir şekilde çalıştığından emin olduktan sonra e-posta hesaplarınızdan bir veya birkaçını, bir ya da birden fazla açık-kişisel anahtar çifti oluşturacak şekilde **Enigmail** kullanmaları için yapılandırabilirsiniz.

### 4.2.1 Anahtar Çifti Oluşturmak için Enigmail Sihirbazı Nasıl Kullanılır?

**Enigmail** açık-kişisel anahtar çifti oluşturmak için iki yol sunar. Birincisi **Enigmail Kurulum Sihirbazı**, ikincisi ise **Anahtar Yönetimi** ekranını kullanır.

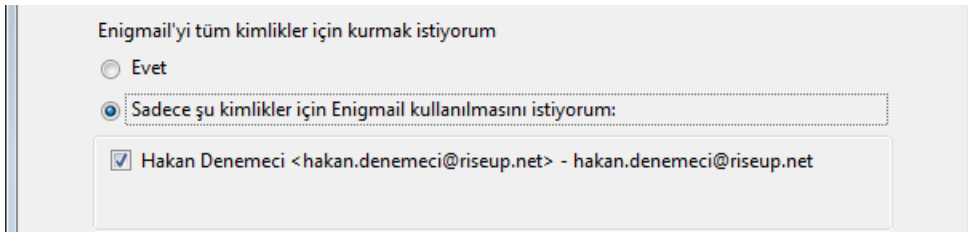
**Enigmail Kurulum Sihirbazı** kullanarak ilk defa anahtar çifti oluşturmak için aşağıdaki adımları takip edin:

**1. Adım. Kurulum Sihirbazı** penceresi henüz etkin değilse **Enigmail > Kurulum Sihirbazı'nı** seçin ve **Enigmail Kurulum Sihirbazı** ekranını aşağıda görüldüğü şekilde açın:



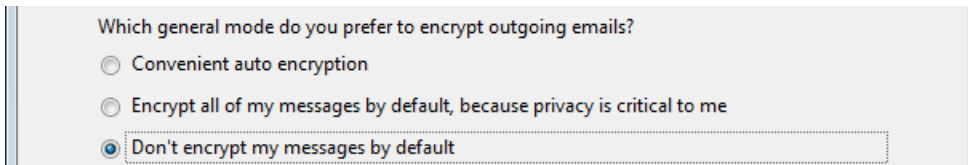
Şekil 9: Enigmail Kurulum Sihirbazı'na Hoşgeldiniz penceresi

**2. Adım.** Aşağıdaki ekranı etkinleştirmek için **İleri >** 'yi **tıklayın**. Bu ekran sadece başka bir hesap için anahtar çiftlemeyi kurmuşsanız açılacaktır.



Şekil 10: Kimlikleri Seç ekranı

**3. Adım.** Aşağıdaki ekranı etkinleştirmek için **İleri >** 'yi **tıklayın**.



Şekil 11: Şifreleme – Giden E-postalarınızı Şifreleyin ekranı

**4. Adım.** Aşağıdaki ekranı etkinleştirmek için **İleri >** 'yi **tıklayın**.

Which general mode do you prefer to sign outgoing emails?

☐ Sign all of my messages by default

☒ Don't sign my messages by default

Şekil 12: İmzalama – Giden E-postalarınızı Dijital Olarak İmzalayın ekranı

5. Adım. Aşağıdaki ekranı etkinleştirmek için **İleri >** yi **tıklayın**.

Enigmail'in makinanızda daha iyi çalışabilmesi için bir kaç seçeneği değiştirmek ister misiniz ?

☒ Evet **Detaylar ...**

☐ Hayır, teşekkürler

Şekil 13: Tercihler – Enigmail'in Daha Düzgün Çalışması İçin E-posta Ayarlarınızı Değiştirin ekranı

6. Adım. Anahtar Yarat – E-postalarınızı İmzalamak ve Şifrelemek için Anahtar Yarat penceresini etkinleştirmek için **İleri >** yi **tıklayın**.

**Not:** Bir e-posta hesabı için ilk defa anahtar yarattığınız zaman, *OpenPGP Anahtarı Bulunamadı* ekranı görünecektir.

7. Adım. E-postamı imzalamak ve şifrelemek için yeni bir anahtar çifti yaratmak istiyorum'u **seçin**.

8. Adım. Her iki Parola alanına güçlü bir parola **girin**.

Hesap / Kullanıcı ID'si:  
Hakan Denemeci <hakan.denemeci@riseup.net> - hakan.denemeci@riseup.net

Parola  
.....

Lütfen tekrar girerek parolanızı doğrulayın  
.....

Şekil 15: Anahtar Yarat – E-postalarınızı İmzalamak ve Şifrelemek için Anahtar Yarat penceresi

9. Adım. Özet ekranını etkinleştirmek için **İleri >** yi **tıklayın**. Bu ekran anahtar çifti oluştururken kullanılan ayarları gösterecektir.

10. Adım. Aşağıda görüldüğü gibi anahtar çifti oluşturmayı başlatmak için **İleri >** yi **tıklayın**:

Enigmail Kurulum Sihirbazı

**Anahtar Oluşturma**  
Anahtarınızı şu an üretiliyor

Anahtar Üretim Konsolu

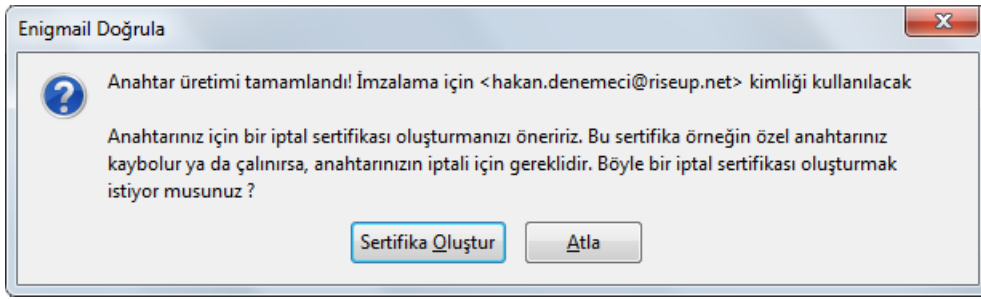
**NOT: Anahtar üretiminin bitmesi biraz zaman alabilir.** Anahtar üretimi sırasında uygulamayı kapatmayın. Aktif olarak internette gezinmek ya da diske ilgili işler yapmak rasgele üretimi kolaylaştıracağından işlemin hızını artıracaktır. Anahtar üretimi bittiğinde uyarılacaksınız.

.....

Şekil 16: Anahtar Oluşturma – Şu anda anahtarınız oluşturuluyor penceresi

**Not:** Enigmail Kurulum Sihirbazı tarafından oluşturulan her anahtar çifti otomatik olarak 4096-bit büyüklüğündedir ve 5 yıllık ömrü vardır.

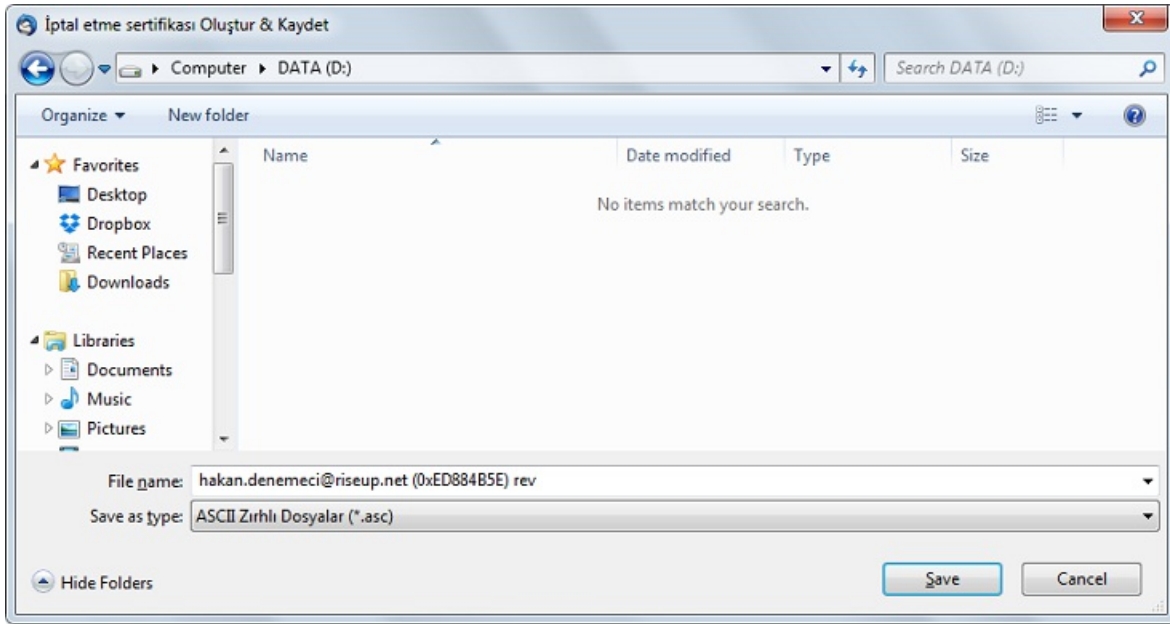
11. Adım. Anahtar oluşturulduktan sonra bir iptal etme sertifikası yaratmak için yönlendirileceksiniz. Aşağıda görüldüğü şekilde **Sertifika Oluştur** ı **tıklayın**:



Şekil 17: Enigmail Onay daveti

**Not:** Zararlı veya kötü niyetli bir tarafın kişisel anahtarınıza izinsiz erişim kazandığını öğrenir veya anahtarınıza erişiminizi kaybederseniz iptal etme sertifikasını iletişimde olduğunuz kişilere gönderebilir ve sizin eşleşmiş Açık anahtarınızı kullanmamaları gerektiğini bildirebilirsiniz. Bilgisayarınızın kaybolması, çalınması veya ele geçirilmesi durumunda da aynı işlemi yapmanız gerekir. İptal sertifikanızı yedeklemenizi ve korumanızı şiddetle öneririz.

**12. Adım.** Yeni oluşturulan anahtarınız ile bağlantılı olan parolanızı **girmeniz** istenecek. Bu işlemten sonra sertifikanızı güvenli bir şekilde saklayacağınız bir yer **seçin** ve takip eden ekranda **Save** i tıklayın.



Şekil 18: İptal Etme Sertifikasını Yarat ve Sakla

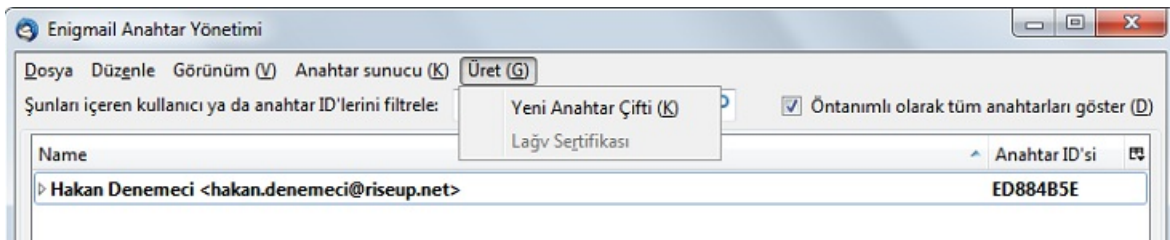
**13. Adım.** Anahtar çiftini ve iptal etme sertifikasını oluşturmayı tamamlamak için **İleri >** i tıklayın.

#### 4.2.2 Başka bir E-posta Hesabı için Nasıl Ek Anahtar Çifti ve İptal Etme Sertifikası Oluşturulur?

Her e-posta hesabı için ayrı bir anahtar çifti oluşturmak yaygın bir yöntemdir. Birden fazla e-posta hesabı için aynı anahtar çiftini kullanmak mümkündür, fakat bu durum iletişimde olduğunuz kişiler için kafa karıştırıcı olabilir. Tek bir anahtar çiftine birden fazla e-posta hesabı eklenebilir (bu konuya bu bölümde değinmiyoruz) ve bunun belli kullanım faydaları vardır, ama bu yöntem tüm bu e-posta hesaplarını tek bir kişi ile ilişkilendirmiş olur ki bu da istenmeyen bir durum olabilir.

Diğer e-posta hesaplarınız için ek anahtar çiftleri oluşturmak istiyorsanız aşağıdaki adımları takip edin.

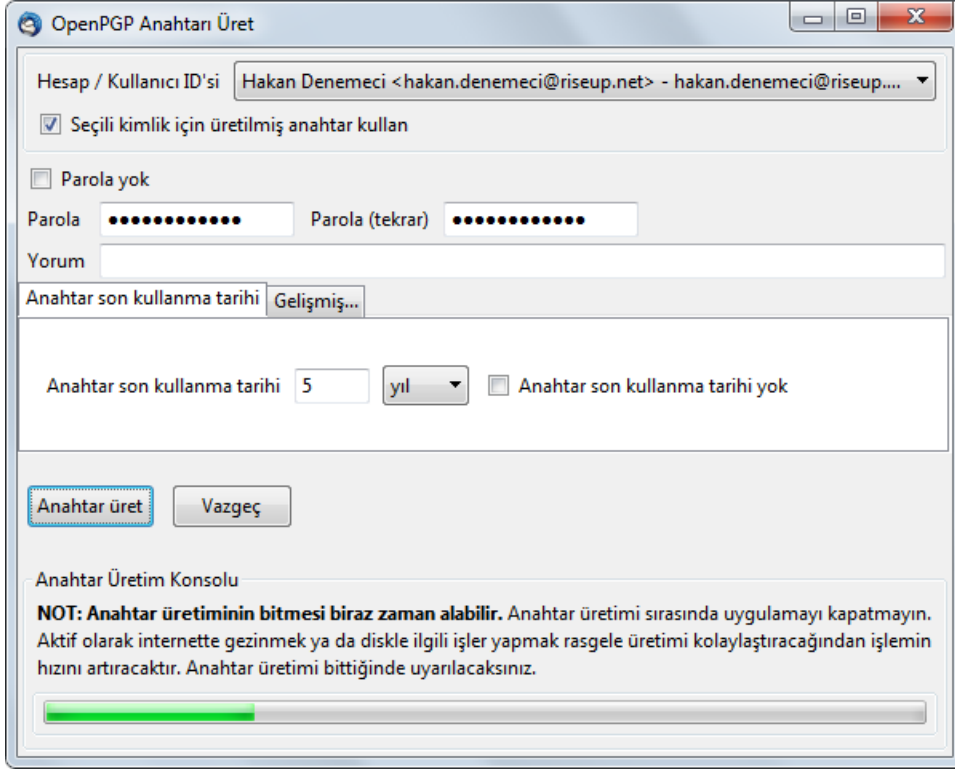
**1. Adım.** Aşağıda görünen ekranı etkinleştirmek için **Enigmail > Anahtar Yönetimi**'ni seçiniz:



Şekil 19: Enigmail Anahtar Yönetimi Oluşturma menüsünde seçilmiş Yeni Anahtar Çifti

**Not:** İlk e-posta hesabınız için **OpenPGP Kurulum Sihirbazı** ile oluşturulan anahtar çiftini görmek için **Varsayılan Tüm Anahtarları Göster**'i **seçin**. Bu ekranı yukarıdaki Şekil 19 ve aşağıdaki Şekil 23'te görebilirsiniz.

**2. Adım.** Yukarıdaki Şekil 19'da görüldüğü gibi *Anahtar Yönetimi'nden Oluştur > Yeni Anahtar Çifti'ni seçin*. Bunu yaptığınız zaman aşağıdaki ekranı göreceksiniz:

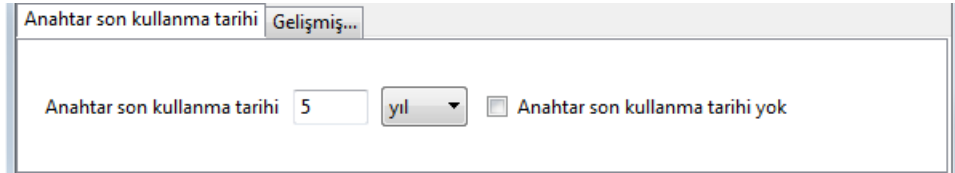
The image shows a window titled "OpenPGP Anahtar Üret". At the top, there is a dropdown menu for "Hesap / Kullanıcı ID'si" with the value "Hakan Denemeci <hakan.denemeci@riseup.net> - hakan.denemeci@riseup....". Below this is a checked checkbox "Seçili kimlik için üretilmiş anahtar kullan". There are two input fields for "Parola" and "Parola (tekrar)" both containing dots. A "Yorum" text area is empty. Below that is a section for "Anahtar son kullanma tarihi" with a dropdown set to "Gelişmiş...", a text input for "5", a dropdown for "yıl", and a checkbox "Anahtar son kullanma tarihi yok". At the bottom left are buttons "Anahtar üret" and "Vazgeç". Below these is a section titled "Anahtar Üretim Konsolu" with a "NOT" message: "NOT: Anahtar üretiminin bitmesi biraz zaman alabilir. Anahtar üretimi sırasında uygulamayı kapatmayın. Aktif olarak internette gezinmek ya da diskle ilgili işler yapmak rasgele üretimi kolaylaştıracağından işlemin hızını artıracaktır. Anahtar üretimi bittiğinde uyarılacaksınız." A green progress bar is shown at the bottom.

Şekil 20: OpenPGP Anahtarı Oluştur ekranı

**3. Adım.** *Açılan Hesap – Kullanıcı Kimliği* listesinden bir e-posta hesabı **seçin** ve *Seçilen kimlik için oluşturulan anahtarı kullan'ı işaretleyin*. Kişisel anahtarınızı korumak için bir parola oluşturun.

**Not:** Parola kullanıcı şifresinden daha uzundur. **Enigmail** sizi sıradan bir kullanıcı şifresinden daha uzun ve daha güvenli bir parola kullanmaya teşvik eder.

**Önemli:** Anahtar çiftlerini her zaman güvenli bir parola ile oluşturun ve **hiçbir zaman** 'parola istemiyorum' seçeneğini etkinleştirmeyin.

The image shows a close-up of the "Anahtar son kullanma tarihi" section. It has a dropdown menu set to "Gelişmiş...", a text input for "5", a dropdown for "yıl", and a checkbox "Anahtar son kullanma tarihi yok".

Şekil 21: OpenPGP Anahtarı Oluştur ekranında seçili Anahtar Zaman Aşımı sekmesi

**Not:** Bir anahtar çiftinin geçerli kalma süresi tamamen sizin gizlilik ve güvenlik ihtiyaçlarınıza bağlıdır. Anahtar çiftlerinizi ne kadar sık değiştirseniz, yeni anahtar çiftinizin tehlike altına girme olasılığı o kadar düşük olur. Bununla birlikte, anahtar çiftinizi her değiştirdiğinizde, iletişimde olduğunuz kişilere açık şifrenizi yeniden göndermeniz ve her biri ile yeniden onaylamanız gerekir.

**4. Adım.** Uygun bulduğunuz sayıyı **tuşlayın** ve anahtarınızın geçerli kalmasını istediğiniz zaman birimini (*gün, ay veya yıl*) **seçin**.

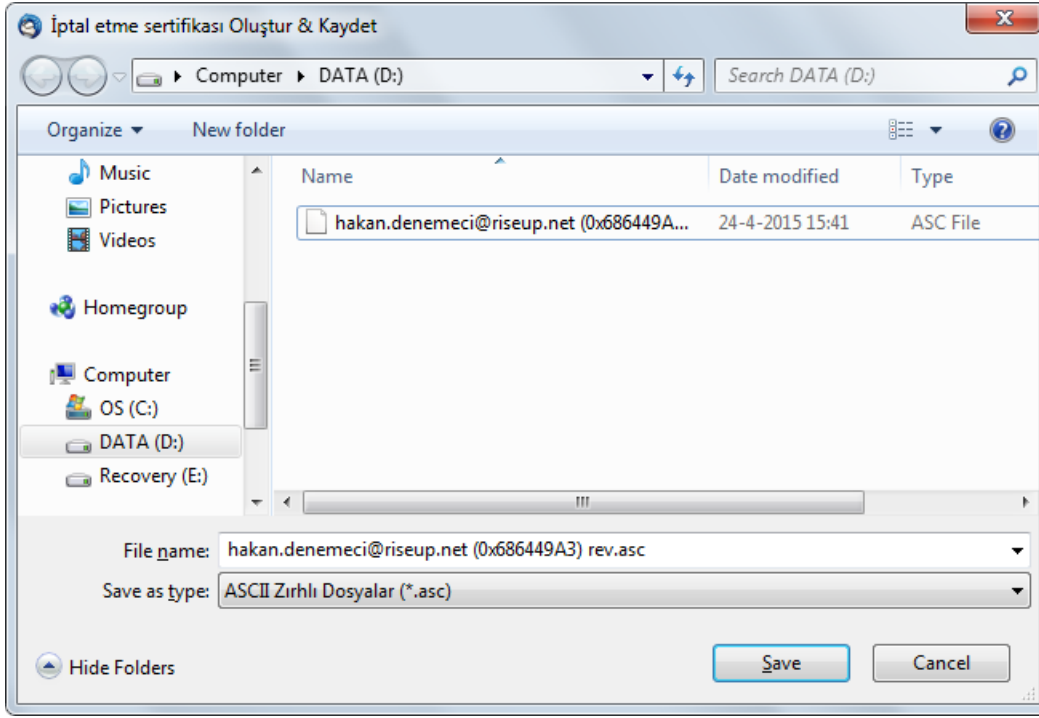
**5. Adım.** Enigmail Onaylama penceresini etkinleştirmek için **Sertifika Oluştur** butonuna **tıklayın**.

**6. Adım.** Şekil 17'de görüldüğü gibi bir sertifika oluşturmak için yönlendirileceksiniz.

**7. Adım.** *İptal Etme Sertifikası Yarat ve Kaydet* gezinim penceresini etkinleştirmek için **Sertifika Oluştur** butonuna **tıklayın**.

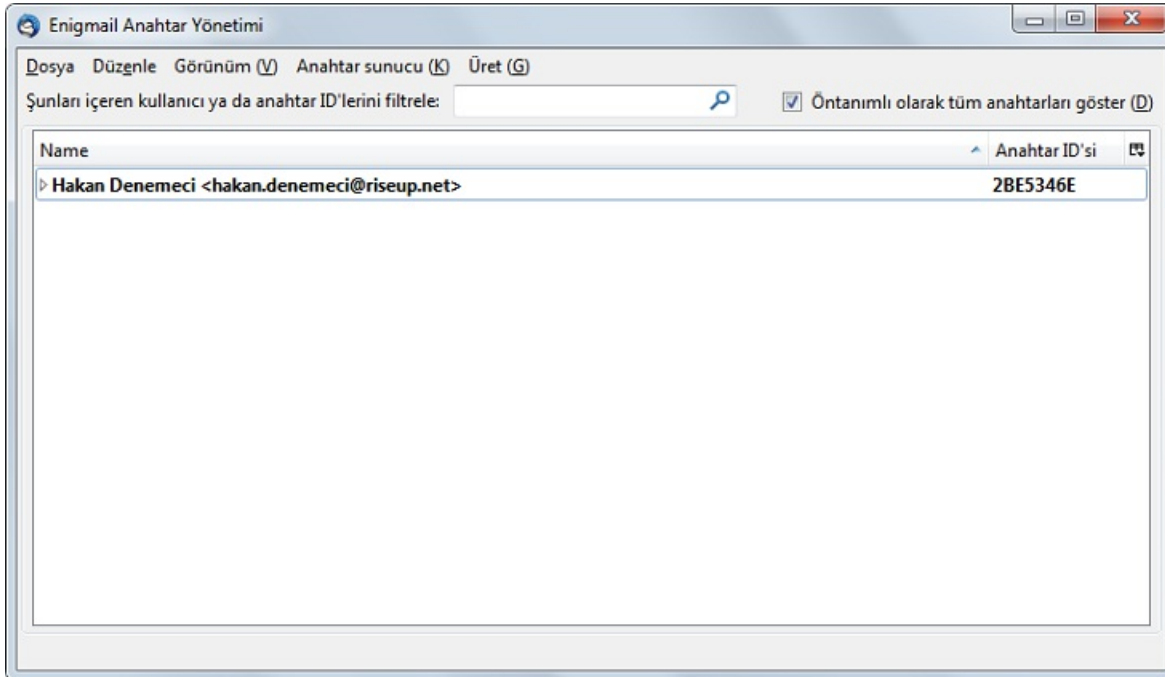
**Not:** Eğer zararlı veya kötü niyetli bir tarafın kişisel anahtarınıza izinsiz erişim kazandığını öğrenir veya anahtarınıza erişiminizi kaybederseniz, iptal etme sertifikasını iletişimde olduğunuz kişilere gönderebilir ve sizin eşleşmiş açık anahtarınızı kullanmamaları gerektiğini bildirebilirsiniz. Bilgisayarınızın kaybolması, çalınması veya ele geçirilmesi durumunda da aynı işlemi yapmanız gerekir. İptal sertifikanızı yedeklemenizi ve korumanızı şiddetle öneririz.

**8. Adım.** Sertifikanızı aşağıdaki ekranda görüldüğü gibi kaydedecek güvenli bir yer seçin ve **Save** butonuna **tıklayın**. Sizden yeni yaratılmış anahtarınız için bir parola girmeniz istenecek.



Şekil 22: İptal Etme Sertifikası Yaratma ve Kaydetme

**9. Adım.** Anahtar çifti ve iptal etme sertifikası oluşturmayı tamamlamak için **Tamam** butonuna tıklayın ve aşağıda görünen ekrana geri dönün:



Şekil 23: Engimail Anahtar Yönetimi penceresinde görünen anahtar çifti

**Not:** Tüm anahtar çiftlerini ve onlarla ilişkili hesapları görüntülemek için *Varsayılan Tüm Anahtarları Görüntüle* seçeneğini seçin. Bunu yaparken güvenli bir ortamda olduğunuzdan emin olun.

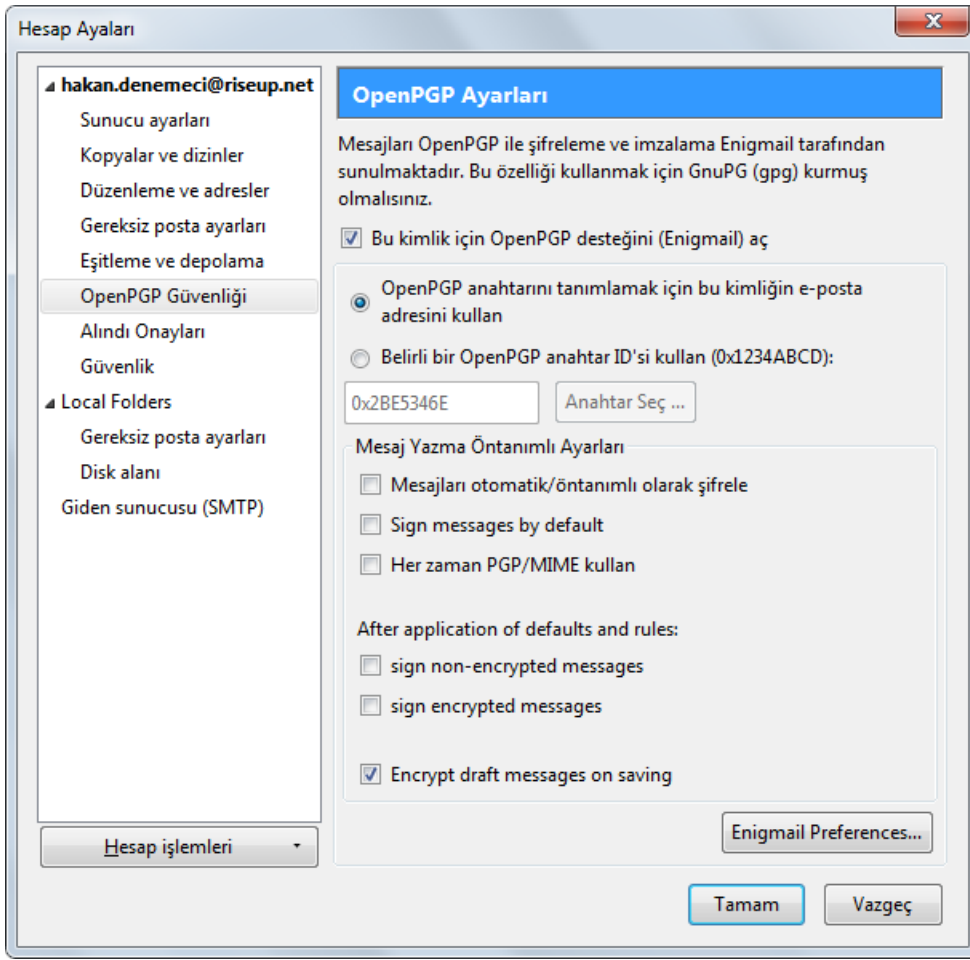
Anahtar çiftinizi ve ona ait iptal etme sertifikasını başarılı bir şekilde oluşturduktan sonra açık şifrelerinizi güvendiğiniz kişilerle paylaşmaya hazırsınız.

### 4.2.3 Enigmail'i E-posta Hesabınız ile Kullanmak için Nasıl Yapılandırılmalısınız?

Enigmail'i belli bir e-posta hesabı ile kullanmak için aşağıdaki adımları takip edin:

**1. Adım.** Thunderbird Menü'sünü açmak için  butonuna tıklayın ve **Seçenekler > Hesap Ayarları**'ni seçin.

**2. Adım.** Kenar çubuğunda *OpenPGP Güvenlik* menüsünü aşağıda görüldüğü gibi seçin:



Şekil 24: Hesap Ayarları - OpenPGP Güvenlik ekranı

**3. Adım.** Bu kimlik için OpenPGP desteğini (Enigmail) aç seçeneğini **işaretleyin** ve OpenPGP anahtarını tanımak için bu kimliğin e-posta adresini kullan seçeneğini **seçin**.

**4. Adım.** Thunderbird konsoluna geri dönmek için **Tamam** butonunu tıklayın.

## 4.3 Açık Anahtarlar Nasıl Karşılıklı Değiş Tokuş Edilir

Birbirinize şifrelenmiş e-posta mesajları göndermeye başlamadan önce, iletişimde olduğunuz kişilerle açık anahtarlarınızı değiş tokuş etmeniz gerekir. Size gelen herhangi bir anahtarı kabul etmeden önce onun gerçekten gönderen kişiye ait olduğunu onaylamanız gerekir.

### 4.3.1 Enigmail Kullanarak Açık Anahtar Nasıl Gönderilir?

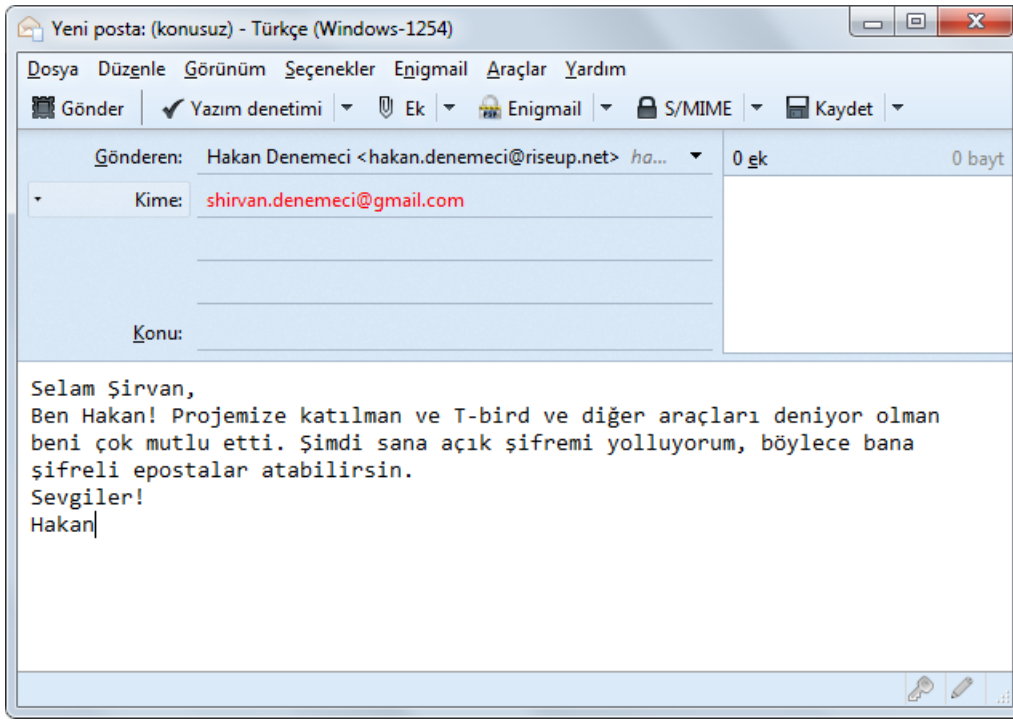
**Enigmail** kullanarak açık anahtar göndermek için sizin ve iletişimde olduğunuz kişinin aşağıdaki adımları takip etmesi gerekir:

**1. Adım.** Thunderbird'ü açın ve yeni bir mesaj yazmak için **Yeni ileti** butonunu tıklayın.

**2. Adım.** Menüden **Enigmail > Açık Anahtarımı Ekle** seçeneğini **seçin**.

**Not:** Bu yöntemde **Eklentiler** bölmesi hemen görünmeyebilir, fakat mesajı gönderdiğiniz anda görünecektir.

Eğer başka bir açık anahtar göndermek isterseniz, menüden **Enigmail > Açık Anahtar Ekle...** seçeneğini **seçin** ve daha sonra göndermek istediğiniz anahtarı **seçin**.



Şekil 25: Eklentiler bölmesindeki eklenmiş açık anahtarı gösteren Mesaj Yaz bölümü.

**3. Adım.** Eklenmiş açık anahtarınız ile e-posta göndermek için **Gönder** butonuna tıklayın.

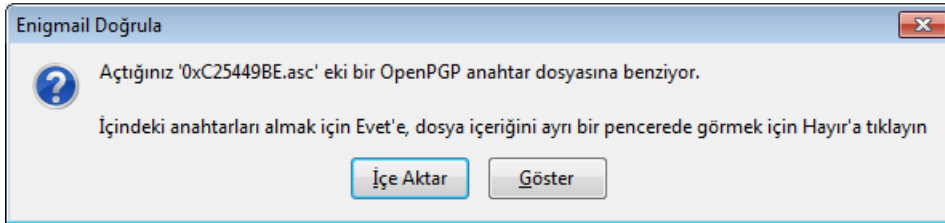
#### 4.3.2 Açık Anahtar Enigmail Kullanarak Nasıl İçeri Aktarılır?

Hem siz hem de iletişimde olduğunuz kişi birbirinizin açık anahtarlarını içeri aktarırken aşağıdaki adımları takip etmelisiniz:

**1 Adım.** İletişimde olduğunuz kişinin açık anahtarını içeren e-postayı **seçin** ve **açın**. Ek şu şekilde görünecektir:

1 attachment: 1 ek: 0x06A170C6.asc 3,1 KB

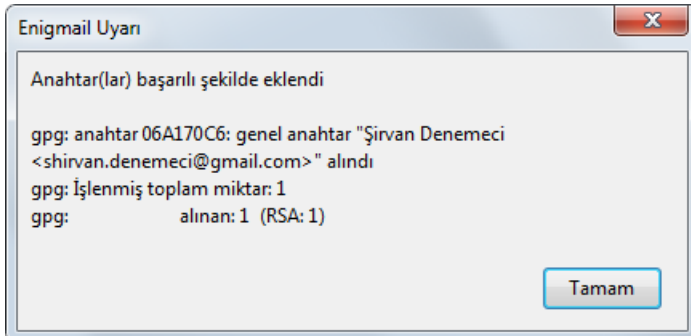
**2. Adım.** 0x06A170C6.asc 3,1 KB dosyasının üstüne görünen ek dosyaya **tıklayın**. **Enigmail** açık anahtar içeren e-postayı tanıyacak ve aşağıda görüldüğü şekilde sizi açık anahtarı içeri aktarmaya davet edecektir:



Şekil 26: Enigmail Açık Anahtarı İçeri Aktarmayı Onayla

**3. Adım.** İletişimde olduğunuz kişinin açık anahtarını içeri aktarmak için **İçer Aktar** butonuna tıklayın.

Açık anahtarı başarılı bir şekilde içeri aktardıysanız, aşağıdakine benzer bir mesaj göreceksiniz:

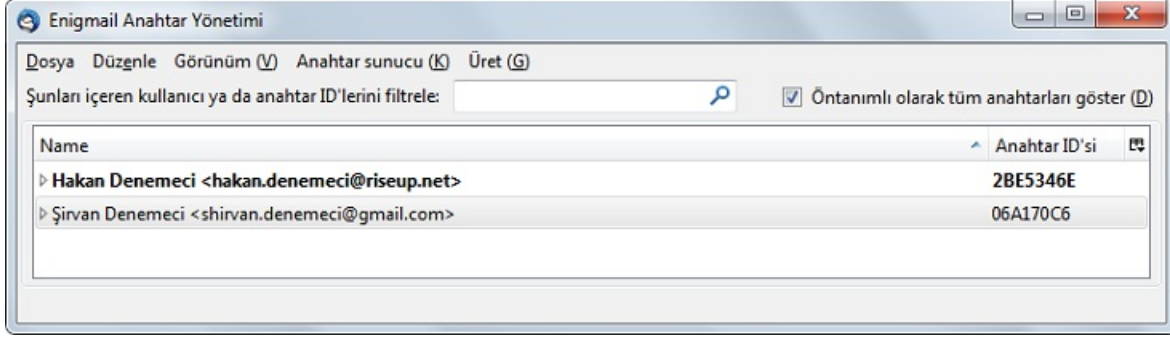


Şekil 27: İletişimde olduğunuz kişinin açık anahtarını gösteren Enigmail Uyarı ekranı

İletişimde olduğunuz kişinin açık anahtarını başarılı bir şekilde içeri aktardığınızı doğrulamak için, aşağıdaki adımı

uygulayın:

**1. Adım.** *Enigmail Anahtar Yönetimi* ekranını aşağıda görüldüğü gibi görüntülemek için **Enigmail > Anahtar Yönetimi**'ni seçin:



Şekil 28: Yeni içeri aktarılmış bir açık anahtarı gösteren Enigmail – Anahtar Yönetimi ekranı

Anahtarları görmek için *Varsayılan Tüm Anahtarları Göster* seçeneğinin seçili olması gerektiğini **unutmayın**.

## 4.4 Bir Anahtar Çifti Nasıl Doğrulandır ve İmzalanır?

Son olarak, içeri aktarılan anahtarın gerçekten de gönderdiği görülen kişi tarafından gönderildiğini doğrulamalı ve geçerliliğinden emin olmalısınız. Bu, gönderilen her açık anahtar için hem sizin hem de e-posta yoluyla iletişimde olduğunuz herkesin uygulaması gereken bir adımdır.

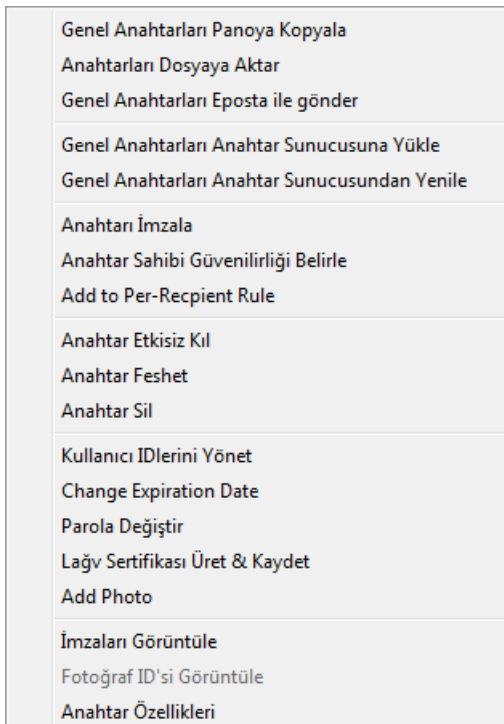
### 4.4.1 Anahtar Çifti Nasıl Doğrulandır?

**1. Adım.** İletişimde olduğunuz kişi ile e-posta olmayan bir yöntem üzerinden **irtibat kurun**. Bu telefon, cep telefonu mesajı, **Voice over Internet Protocol (VoIP)** veya herhangi başka bir yöntem olabilir, fakat her durumda doğru kişi ile görüştüğünüzden **tamamıyla emin olun**. Bu bakımdan, eğer imkânınız varsa ve güvenli bir şekilde ayarlayabiliyorsanız ses veya video görüşmeleri veya yüz yüze görüşmeler en uygun yöntemlerdir.

**2. Adım.** Hem siz hem de iletişimde olduğunuz kişi değişik tokuş ettiğiniz açık anahtarların 'parmak izlerini' doğrulamalıdır. Parmak izi, her anahtarı belirleyen özgün sayı ve harf dizilerinden oluşur. Yarattığınız ve içeri aktardığınız anahtar çiftlerinin parmak izlerini görmek için **Enigmail Anahtar Yönetimi** ekranını kullanabilirsiniz.

Bir anahtar çiftinin parmak izlerini görmek için aşağıdaki adımları takip edin:

**1. Adım.** **Enigmail > Anahtar Yönetimi**'ni seçin ve açılır menüyü etkinleştirmek için belli bir anahtarın üzerine **sağ tıklayın**.



Şekil 29: Enigmail Anahtar Yönetimi menüsünde seçili Anahtar Özellikleri

**2. Adım.** Aşağıdaki ekranı etkinleştirmek için **Anahtar Özellikleri** maddesini **seçin**:

**Anahtar Özellikleri**

Birincil Kullanıcı ID'si: hakan.denemeci <hakan.denemeci@riseup.net>

Anahtar ID'si: 0xF76A5A65

Tip: anahtar çifti

Anahtar doğruluğu: ultra

Güvenilirlik: ultra

Parmakizi: AAE7 E150 9698 64D8 9E89 016A 8800 9DB2 F76A 5A65

Ek Kullanıcı ID'leri: Doğru

| Anahtar Parçası | ID         | Algorit... | Boy... | Oluşturul... | Son Kulla...  |
|-----------------|------------|------------|--------|--------------|---------------|
| özel anahtar    | 0xF76A5A65 | RSA        | 4096   | 20-3-2015    | 18-3-2020 ... |
| altanahtar      | 0x506046D6 | RSA        | 4096   | 20-3-2015    | 18-3-2020 ... |

İşlem Seç ...

Kapat

Şekil 30: Anahtar Özellikleri ekranı

İletişimde olduğunuz kişi de aynı adımları takip etmelidir. Parmak izlerini doğrulamak için, kendi anahtarınızın parmak izlerini iletişimde olduğunuz kişiye okuyun ve onun almış olduğu açık anahtardaki parmak izleri ile aynı olduğunu doğrulamasını isteyin. Daha sonra, iletişimde olduğunuz kişiden aynısını kendi anahtarlarının parmak izleri için yapmasını isteyin. Eğer parmak izleri birbirleri ile uyumlu değilse, açık anahtarlarınız yeniden değiş tokuş edin ve doğrulama işlemini yeniden yapın.

**Not:** Parmak izinin kendisi gizli tutulmak zorunda değildir ve doğrulama işlemini daha sonra yapmak üzere kaydedilebilir.

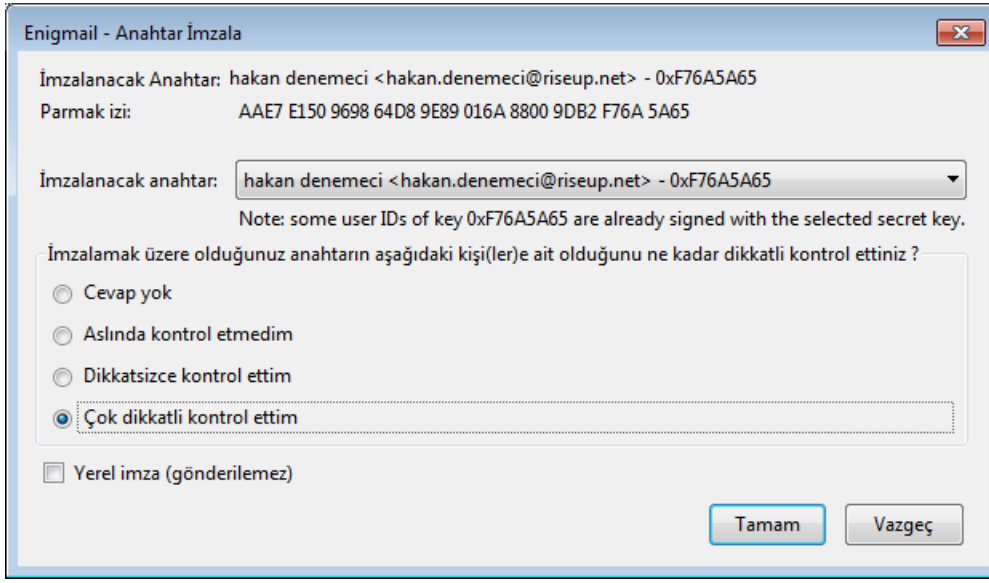
#### 4.4.2 Doğru bir Açık Anahtar Nasıl İmzalanır

İletişimde olduğunuz kişinin anahtarını doğruladıktan sonra, bu anahtarı geçerli kabul ettiğinizi belirtmek için onu *imzalayabilirsiniz*. Anahtarları imzalamak, imzalanmış anahtarı başkasına gönderdiğiniz veya anahtar dağıtıcısına aktardığınız zaman siz ve iletişimde olduğunuz kişi arasındaki bağı görünür hale getirebilir. Bu durumu engellemek için her zaman aşağıdaki *Yerel İmza* seçeneğini seçin.

Doğrulanmış bir açık anahtarı imzalamak için aşağıdaki adımları takip edin:

**1. Adım.** *Anahtar Yönetimi* ekranını açmak için **Enigmail > Anahtar Yönetimi**'ni seçin.

**2. Adım.** *Anahtar Yönetimi* ekranından (bkz. yukarıdaki Şekil 29) iletişimde olduğunuz kişinin açık anahtarına **sağ tıklayınız** ve menüden aşağıdaki ekranı etkinleştirmek için **Anahtarı İmzala** maddesini **seçin**:



Şekil 31: Enigmail – Anahtarı İmzala ekranı

**3. Adım.** *Çok dikkatle kontrol ettim* seçeneğini **işaretleyin**, *Yerel imza (dışarı aktarılamaz)* seçeneğini **seçin** ve iletişimde olduğunuz kişinin açık anahtarını imzalamak için **Tamam**’ı **tıklayın**.

#### 4.4.3 Kendi Anahtar Çiftinizi Nasıl Yönetirsiniz?

*Enigmail Anahtar Yönetimi* ile birbirinden farklı anahtar çiftleri oluşturabilir, onları doğrulayabilir ve imzalayabilirsiniz. Bununla birlikte, başka anahtar yönetimi işlemlerini de gerçekleştirebilirsiniz (bkz. yukarıdaki Şekil 29).

- **Kullanıcı Kimliklerini Yönet** bir anahtar çiftine birden fazla e-posta adresi bağlamanızı sağlar.
- **Son Kullanma Süresini Değiştir** anahtar çiftinizin son kullanma süresini değiştirmenizi sağlar.
- **Parolayı Değiştir** anahtar çiftinizi koruyan parolayı değiştirmenizi sağlar.
- **İptal Etme Sertifikası Oluştur ve Sakla**

## 4.5 Bir Mesaj Nasıl Şifrelenir ve Bir Mesajın Şifresi Nasıl Çözülür?

**Önemli:** E-posta mesajlarının başlığı – *Konu* kısmı, gönderilen kimselerle ilgili bilgi ve **To**, **CC** ve **BCC** alanlarındaki bilgiler - *şifrelenemez* ve açık metin olarak gönderilir. E-posta iletişimlerinin gizliliğini ve güvenliğini sağlamak için e-postanızın konu kısmına hassas bilgiler ve e-postanın içeriğini belli edecek tanımlar eklenmemelidir. Ek olarak, bir grup insana e-posta gönderirken tüm adresleri BCC alanına koymanız tavsiye edilir.

Ek dosyaları bulunan e-posta mesajlarını şifrelerken, **PGP/MIME** seçeneğini kullanmanızı şiddetle tavsiye ederiz. Bu seçenek, e-postanıza eklenmiş olan tüm dosya ve dosya isimlerini de kapsayacak bir şifrelemeyi mümkün kılar.

Thunderbird/Enigmail/GnuPG kullanarak gönderdiğiniz tüm şifreli e-postalar otomatik olarak sizin ve bu e-postanın alıcılarının anahtarları üzerinden şifrelenir ve bu sayede e-postalarınızın şifresini gidenler dosyasında çözebilirsiniz.

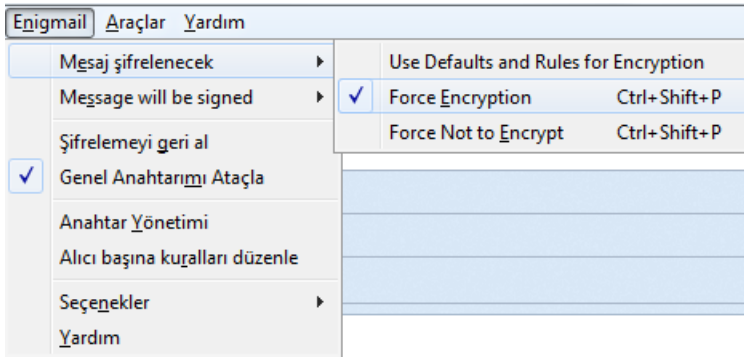
### 4.5.1 Bir Mesajı Nasıl Şifreleyebilirsiniz

Hem siz hem de iletişimde olduğunuz kişi birbirinizin açık anahtarlarını başarılı bir şekilde içeri aktarıp doğruladıktan ve imzaladıktan sonra, şifreli mesajlar göndermeye ve gelen mesajların şifrelerini çözmeye hazır durumdasınız demektir.

Gönderdiğiniz e-posta mesajının içeriğini şifrelemek için aşağıdaki adımları takip edin:

**1. Adım.** Thunderbird’ü açın ve e-posta oluşturmak için **Yeni ileti**’yi **tıklayın**.

**2. Adım.** Mesajı şifreli hale getirmek için *Enigmail* > *Mesaj şifrelenmeyecek* seçeneğine **tıklayın** ve aşağıdaki ekranda görüldüğü gibi **Yeni ileti**’yi **seçin**:



Şekil 33: Şifrelemeyi Zorla seçeneği

**3. Adım.** Mesajı imzalamak için *Enigmail* > *Mesaj imzalanmayacak* seçeneğine **tıklayın** ve *Zorla İmzala*'yı **seçin**.

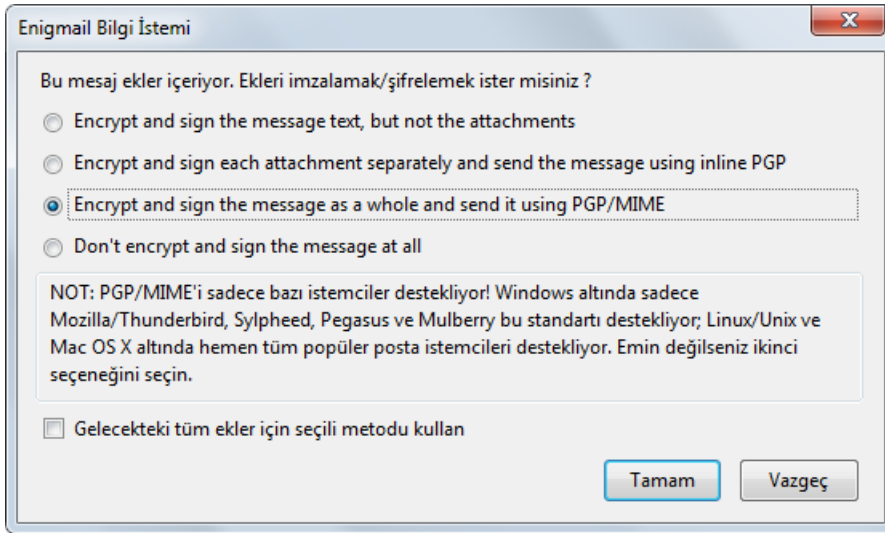
**Not:** Mesajınızın şifrelenmiş ve imzalanmış olduğunu doğrulamak için, Enigmail araç çubuğunda iki ikonun aşağıda görüldüğü gibi **seçili** olduğundan emin olun:



Şekil 34: Şifreleme ve imzalama etkinleştirilmiş

**4. Adım.** Mesaj göndermek için **Gönder** butonuna **tıklayın**. Mesajı imzalarken kişisel anahtarınızı kullanmak için parolanızı girmeniz istenebilir.

**İsteğe Bağlı 5. Adım.** Eğer mesajınıza bir dosya ekliyorsanız, *Tüm Mesajı Şifrele/İmzala PGP/MIME kullanarak yolla* seçeneğini **seçin** ve daha sonra **Tamam**'ı tıklayın:

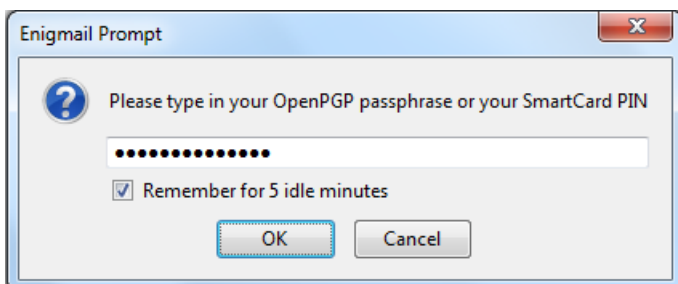


Şekil 35: Enigmail Bilgi ekranı

**Not:** Her ek dosyayı ayrı olarak şiflerseniz (yukarıdaki Şekil 35'teki ikinci seçenek), eklenen dosyaların isimleri şifrelenmez ve oldukları gibi görünürler! Bu hassas bilgilerin yayılmasına neden olabilir! PGP/MIME kullanmak, e-posta metninin, tüm ek dosyaların ve isimlerinin şifrelenmiş ve gizli tutulması için çok önemlidir.

#### 4.5.22 Bir Mesajın Şifresi Nasıl Çözülür?

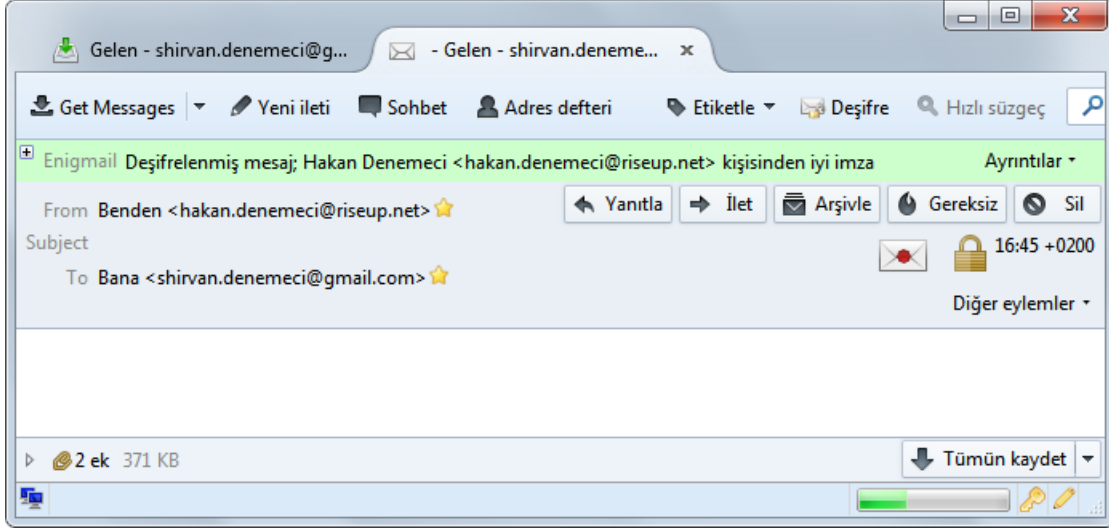
Şifrelenmiş bir mesaj aldığınız ve açtığınız zaman, **Enigmail/OpenPGP** otomatik olarak bu mesajın şifresini çözmeye çalışacaktır. Eğer bu işlem başlamazsa **Şifre Çöz** tuşuna basın ve aşağıdaki ekranın etkinleştiğini görün:



Şekil 36: Enigmail Bilgi – Lütfen OpenPGP parolanızı veya SmartCard PIN'inizi girin

**1. Adım.** Yukarıda görüldüğü gibi parolanızı **girin**.

Kişisel anahtar parolanızı girdikten sonra, mesajın şifresi çözülür ve aşağıdaki gibi görünür:



Şekil 37: Mesaj bölümünde henüz şifresi çözülüş mesaj

Mesajın şifresini başarı ile çözdünüz. **4.5 Şifrelenmiş E-Posta Mesajları Nasıl Gönderebilirsiniz ve E-posta Mesajlarının Şifresini Nasıl Çözebilirsiniz?** Bölümünde belirtilen adımları her mesaj değişik tokuşunda takip ederek, e-posta değişik tokuşlarınızın gözlenmesini engelleyerek, gizli ve kimlik denetimi yapılmış bir iletişim kanalı oluşturabilir ve bu kanalı kalıcı hale getirebilirsiniz.

### 4.5.3 Güvenlik Seçeneklerini Genişletmek

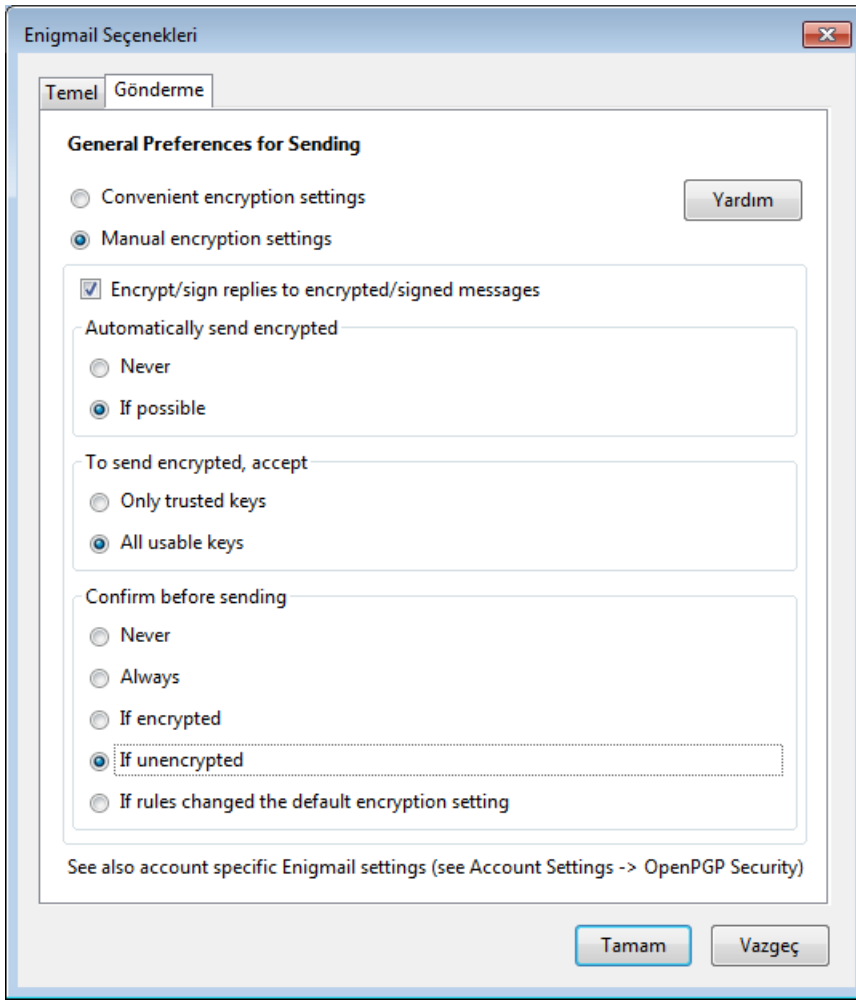
Gizliliğinizi korumak için *Enigmail* ve *GnuPG* kullanırken, gönderdiğiniz **her** e-postanın şifreli olması çok önemlidir. Bu durum, özellikle, gelen şifreli e-postalara yazılan cevaplar, daha sonra şifreleyeceğiniz e-posta taslakları ve şifrelenmiş e-postalardan yapılan alıntılar için geçerlidir.

**Her zaman, mesaj şifrelemeyi mesajı yazmaya başlamadan önce etkinleştirin (4.5.1 Bir Mesajı Nasıl Şifreleyebilirsiniz? bölümünde anlatıldığı şekilde).** Bu şekilde, mesajlarınızın taslaklarının da e-posta dağıtıcısına şifrelenmiş bir şekilde girildiğinden emin olursunuz.

Ek olarak, **Enigmail'i şifrelenmemiş bir mesajı göndermeden önce sizi uyaracak şekilde yapılandırmanızı** şiddetle tavsiye ederiz. Aşağıdaki adımlar bunu nasıl yapacağınızı gösteriyor:

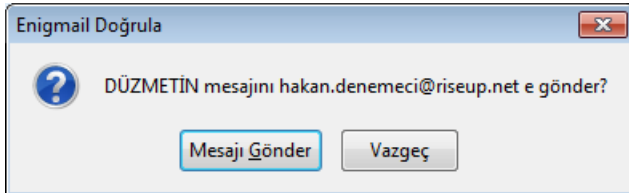
**1. Adım.** *Enigmail* > *Tercihler* menüsüne **tıklayın** ve *Gönderme* sekmesini **seçin**.

**2. Adım.** *Şifrelenmemiş ise - Göndermeden önce onayla'yı* **seçin** ve *Tamam'ı* tıklayın.



Şekil 38: Enigmail Tercihler – Göndermeden önce onayla

Şifrelenmemiş her e-postayı göndermeden önce, şifrelenmemiş bir e-posta gönderiyor olduğunuza dair aşağıda görüldüğü şekilde uyarılacaksınız. E-postayı şifrelemek istiyorsanız, *iptal et'i tıklayın* ve yukarıdaki 4.5.1 bölümündeki adımları takip edin.



Şekil 39: Enigmail Onay

Konu, Kime, CC ve BCC kısımlarındaki bilgilerin **hiçbir zaman** şifrelenmediğini **unutmayın**.

## GPG ve Enigmail ile Taşınabilir Thunderbird

### Short Description:



**Mozilla Thunderbird** e-posta almanızı, göndermenizi ve saklamanızı sağlayan ücretsiz ve açık kaynak e-posta istemcisidir. Tek bir programla farklı e-posta hesaplarınızı yönetebilirsiniz. **Enigmail** ve **GnuPG** size kimlik doğrulama, dijital imzalama ve şifreleme imkanı vererek e-posta iletişiminizin gizliliğini ve güvenliğini sağlar.

## 5.1 Thunderbird'ün Kurulumlu ve Taşınabilir Versiyonları Arasındaki Farklar

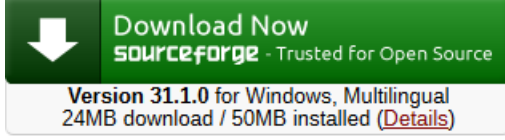
**Taşınabilir Thunderbird'ü** kullanmanın en önemli faydası e-postalarınızın yerel kopyalarınızı çıkarılabilir sürücü ya da

USB bellek çubuğuna kaydedebilmelisiniz. Buna ek olarak, hem Taşınabilir Thunderbird programı hem de e-postalarınızın bütün yerel kopyaları **TrueCrypt** tarafından şifrelenmiş disk bölümü içinde saklanabilir. Bu sayede, e-postalarınızın güvenliğini geliştirir ve e-posta hesaplarınızı ve kullandığınız adresleri saklayabilirsiniz. Fakat unutmayın ki harici aygıtınız ya da USB bellek çubuğunuz ve de taşınabilir araçlarınız sadece kullandığınız bilgisayar kadar güvenlidir, ve reklam destekli yazılımlar, kötü niyetli yazılımlar, casus yazılımlar ve virüslere maruz kalma riskini taşıyabilirler.

**Not:** E-posta iletişiminizin gizlilik ve güvenliğini korumak için, bu sayfanın sonunda açıklandığı gibi **GnuPG Portable**'i indirip çıkartmanızı şiddetle tavsiye ediyoruz.

## 5.2 Taşınabilir Thunderbird Nasıl İndirilip Çıkartılır?

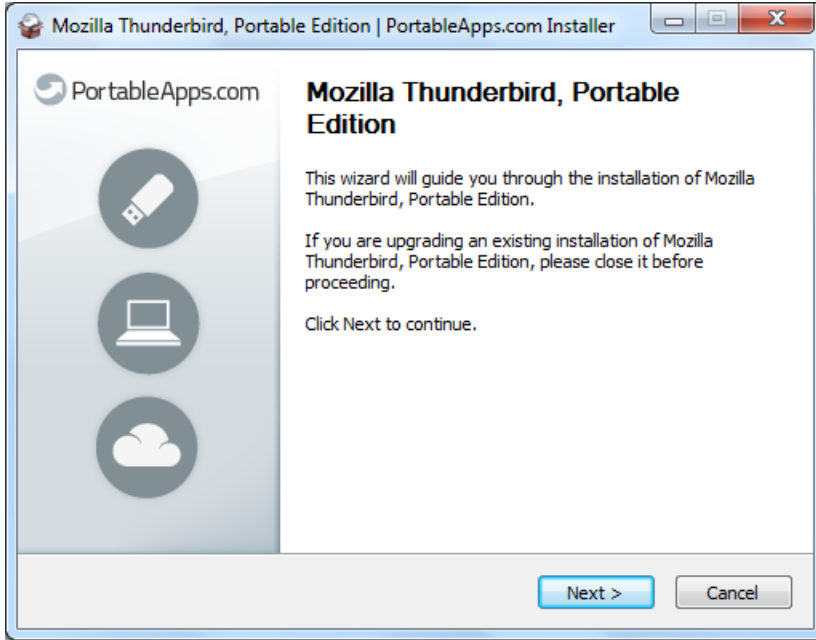
1. Adım. [http://portableapps.com/apps/internet/Thunderbird\\_portable](http://portableapps.com/apps/internet/Thunderbird_portable) <sup>[187]</sup>'i **tıklayarak** ilgili indirme sitesini açın.



2. Adım. **tıklayarak** Source Forge indirme sitesini etkinleştirin.

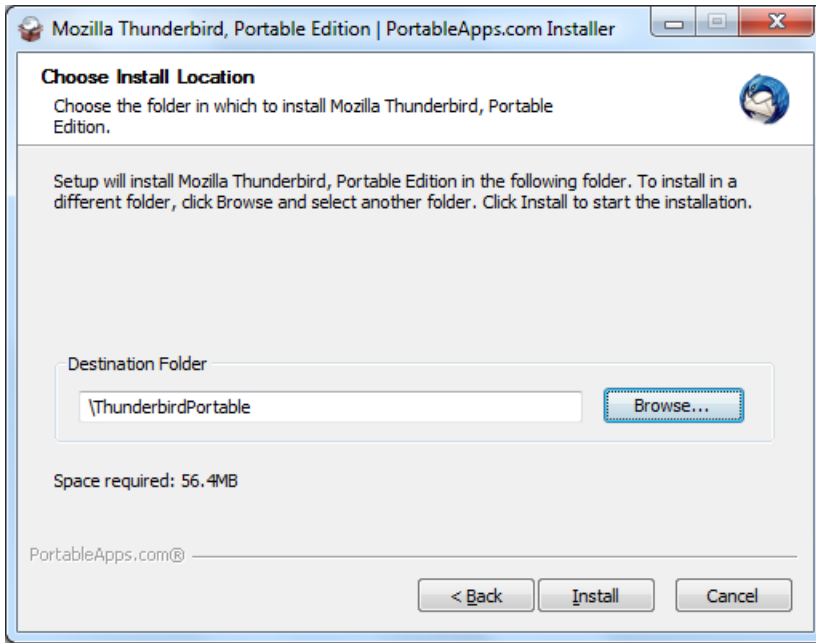
3. Adım. **tıklayarak** ThunderbirdPortable\_31.1.0\_English.paf.exe kurulum dosyasını bilgisayarınıza kaydedin ve onu içine indirdiğiniz dosyayı **bulun**.

4. Adım. ThunderbirdPortable\_31.1.0\_English.paf.exe'yi **çift tıklayın**; Dosyayı Aç - Güvenlik Uyarısı kutusu açılabilir. Açılırsa **tıklayarak** aşağıdaki ekranı etkinleştirin:



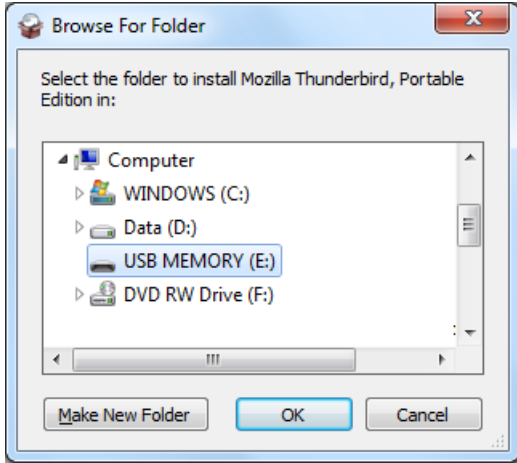
Şekil 1: Mozilla Thunderbird Taşınabilir Sürüm | Portableapps.com Kurucu penceresi

5. Adım. **tıklayarak** aşağıdaki ekranı etkinleştirin:



Şekil 2. Kurulum Yerini Seçiniz penceresi

6. Adım. **Browse...** butonunu tıklayarak aşağıdaki gibi *Dosya Tarama* penceresini etkinleştirin:



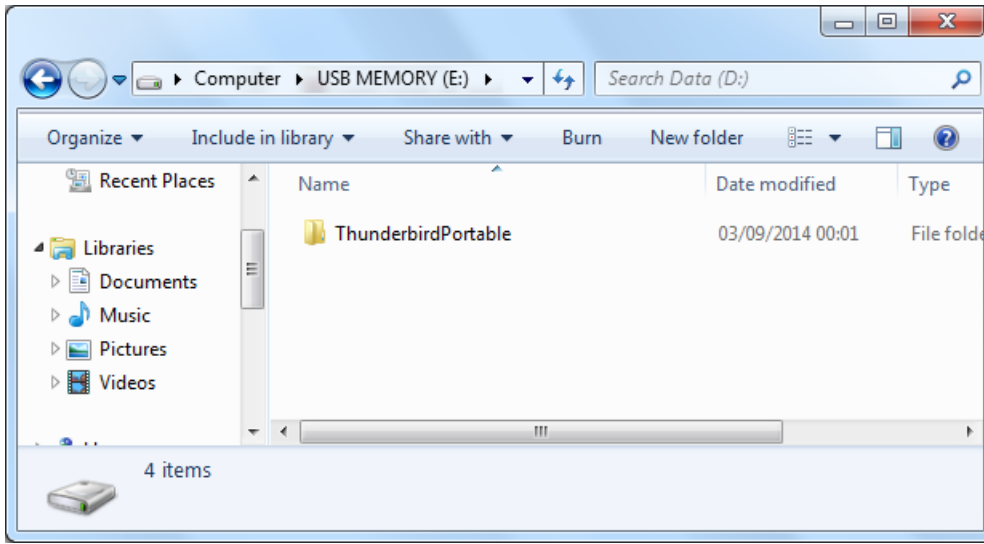
Şekil 3: Dosya Tarama penceresi

7. Adım. Yukarıdaki Şekil 3'te görüldüğü gibi harici sürücünüz ya da USB bellek çubuğunuzdaki hedef dosyaya **ilerleyin**, daha sonra **OK** butonunu tıklayarak **Mozilla Thunderbird, Taşınabilir Sürüm**'ün yerini onaylayın ve *Kurulum Yerini Seçiniz* penceresine geri dönün.

8. Adım. **Install** butonunu tıklayarak *Kurulum* penceresini etkinleştirin ve **Mozilla Thunderbird, Taşınabilir Sürüm** dosyasının çıkartılmasını bekleyin, ve sonrasında **Finish** butonunu tıklayarak çıkartım işlemini bitirin.

9. Adım. **Mozilla Thunderbird, Taşınabilir Sürüm** dosyasının kaydedildiği kaldırılabilir sürücü ya da USB bellek çubuğuna doğru **ilerleyin**.

10. Adım. Kaldırılabilir aracınıza ya da USB bellek çubuğunuza **çift tıklayın**, şöyle bir görüntü karşınıza çıkmalı:



Şekil 4. Mozilla Thunderbird Taşınabilir Sürümü gösteren Thunderbird Taşınabilir dizini

### 5.3 Thunderbird için Taşınabilir GPG Nasıl İndirilir ve Çıkartılır?

1. Adım. [http://portableapps.com/support/thunderbird\\_portable#encryption](http://portableapps.com/support/thunderbird_portable#encryption) <sup>[188]</sup> tıklayarak indirme sitesine yönlendirilir.

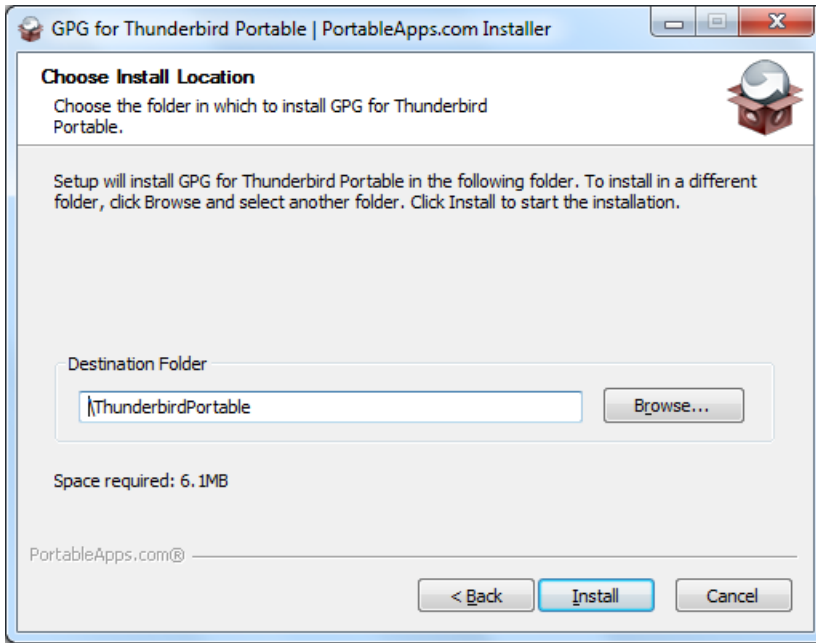
2. Adım. [GPG for Thunderbird Portable 1.4.16](#)'yı tıklayarak, [GPG\\_for\\_Thunderbird\\_Portable\\_1.4.16.paf.exe](#)'yi indirme penceresini etkinleştirin ve sonra [Save File](#) i tıklayarak [GPG\\_for\\_Thunderbird\\_Portable\\_1.4.16.paf.exe](#) kurulum dosyasını kaydedin ve dosyayı kaydettiğiniz yere ilerleyin.

3. Adım. [GPG\\_for\\_Thunderbird\\_Portable\\_1.4.16.paf.exe](#), yi çift tıklayın; Dosyayı Aç – Güvenlik Uyarısı kutusu açılabilir. Açılırsa [Run](#) i tıklayarak aşağıdaki ekranı etkinleştirin:

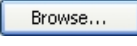


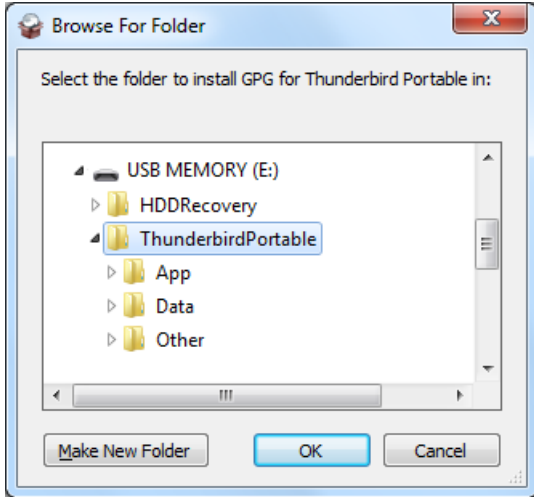
Şekil 5: Kurulum Dili Penceresi

4. Adım. [OK](#) i tıklayarak Thunderbird için **GPG | Taşınabilir Uygulamalar Kurucusu** penceresini etkinleştirin, ve sonrasında [Next >](#) i tıklayarak aşağıdaki ekranı etkinleştirin:

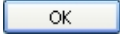
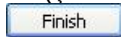


Şekil 6: Kurulum Yerini Seçiniz penceresi

5. Adım.  ı tıklayarak aşağıdaki gibi Dosyayı Tara penceresini etkinleştirin:



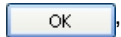
Şekil 7: Dosyayı Tara penceresi

6. Adım. Taşınabilir Thunderbird'ü yüklediğiniz dizine ilerleyin,  ı tıklayarak Kurulum Yerini Seçiniz penceresine (Şekil 7) geri dönün ve sonra  ı tıklayarak Taşınabilir GnuPG'yi çıkarmaya başlayın ve bu işlem bittiğinde  ı tıklayın.

## 5.4 Enigmail Nasıl İndirilir ve Kurulur?

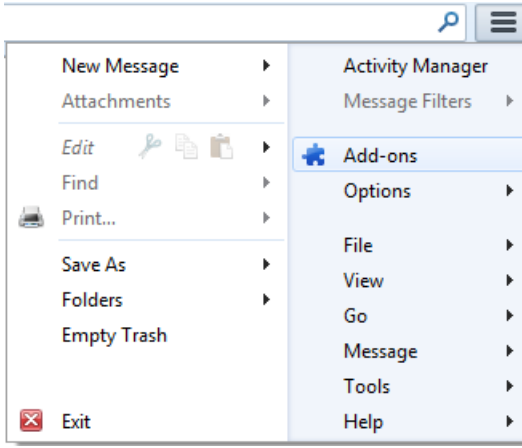
**Enigmail** e-posta iletişiminizin gizliliğini korumanızı sağlayan bir **Mozilla Thunderbird** eklentisidir. **Enigmail** basitçe **GnuPG** şifreleme programını **Thunderbird** içinde kullanmanızı sağlayan bir arayüzdür. **Enigmail** arayüzü **Thunderbird** konsol çubuğunda görünür.

1. Adım. <https://www.enigmail.net/download/> <sup>[189]</sup> ı tıklayarak indirme sitesine yönlendirilin.

2. Adım. İşletim sisteminiz nedir? (mesela Windows) ve Hangi e-posta istemcisini kullanıyorsunuz? (mesela Thunderbird 31) sorularını cevaplandırın ve **enigmail-1.7.2-tb-win.xpi**'yi indirme penceresini etkinleştirmek için **Enigmail x.x.x'i** (mesela 1.7.2) **İndir** linkini tıklayın ve sonrasında  ı tıklayarak (/sbox/screen/thunderbirdportable-en-1/26.png)'i bilgisayarınıza kaydedin.

3. Adım. **Thunderbird Taşınabilir** dizinini açın ve  **ThunderbirdPortable.exe** 'yi çift tıklayarak **Thunderbird Taşınabilir**'i açın.

4. Adım.  'ü tıklayarak **Thunderbird Menü'sünü** görüntüleyin ve aşağıda görüldüğü gibi **Thunderbird Taşınabilir** ana konsolunda **Eklentileri seçin**:



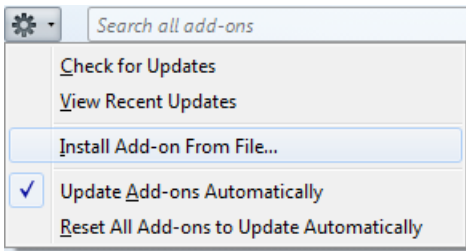
Şekil 8: Eklentiler öğesi seçilmiş Thunderbird Taşınabilir ana konsolu

Bu aşağıdaki ekranı etkinleştirecektir:



Şekil 9: Thunderbird Taşınabilir Eklentiler penceresi

**5. Adım.** Ana Eklentiler bölümünde Enigmail Eklentisi beliriorsa **Install Now** butonuna tıklayın. Belirmiyorsa **Settings** butonuna tıklayın ve **Eklenti Dosyasından Kur'u** aşağıda görüldüğü gibi seçin.



Şekil 10: Eklentiler için Araçlar menüsü

**6. Adım.** Enigmail eklentisini kaydettiğiniz dizine (büyük ihtimalle *İndirilenler* Dizinine) **ilerleyin** ve **Enigmail** eklenti dosyasını **seçin**.

**7. Adım.** Yazılım Kurulumları dizininde **Install Now** butonuna tıklayın.

**8. Adım.** **Restart Now** butonuna tıklayarak Enigmail kurulumunu tamamlayın ve **Thunderbird Taşınabilir'i** tekrar başlatın.

Bütün bu adımları tamamladıktan sonra, lütfen **Thunderbird** [55] bölümüne bakarak e-posta hesaplarınızı kaydetmek ve programı yapılandırmakla devam edin.

#### Offline Installation Instructions :

#### GPG ve Enigmail ile Thunderbird'ü Kurma

- Kısa [Uygulamalı-Rehber'in](#) [1] Giriş bölümünü okuyun
- Aşağıdaki **Thunderbird**, **GPG** ve **Enigmail** ikonlarına **tıklayın** ve kurucuları 'Açın' ya da 'Çalıştırın'. Gerekirse önce

kurucuyu indirin ve sonra yerini bulup üstüne çift tıklayın

- Devam etmeden önce bir sonraki kısımdaki 'Kurulum Yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulumdan sonra silebilirsiniz

Thunderbird: Enigmail: GnuPG:



[190]

ENIGMAIL

[174]



[191]

## Torbirdy- Thunderbird'e dijital anonimlik ve atlatmayı ekleme

Short Description:



**TorBirdy** Tor Ağı üzerinden e-posta göndermek ve almak için kullanabileceğiniz, ve bu sayede kullandığınız e-posta sunucusuyla iletişiminizi koruyan, iletilerinizin anonimliğini artıran ve sansürü atlatan yetisi veren bir **Thunderbird** eklentisidir. **TorBirdy Enigmail** ve **GnuPG** şifrelemesine mükemmel bir ektir.

TorBirdy'yi Mozilla Thunderbird eklentiler sunucusundan [indirebilirsiniz](#) [163].

TorBirdy'yi kullanabilmeniz için aşağıdaki bileşenlerin çalıştırılması ve bilgisayarınızda yapılandırılması gereklidir:

- Thunderbird (lütfen [Enigmail ve GPG'li Thunderbird - Güvenli E-posta İstemcisi](#) [55] bölümüne bakınız);
- Tor Tarayıcısı (lütfen [Tor Tarayıcısı – Dijital Anonimlik ve Atlatma](#) [192] bölümüne bakınız).

Not edilmelidir ki TorBirdy hala geliştirilme ve test edilme aşamasında kabul edilmektedir. VPN veya SSH vekil sunucusu gibi Thunderbird ile e-posta sunucunuz arasındaki iletişimi korumak için kullanılabilecek alternatif metodlar da mevcuttur. Lütfen Nasıl Yapmalı Kitapçığının 8. bölümüne bakınız: [8. İnternette nasıl anonim kalınır ve internet sansürü nasıl aşılr](#)

[75].

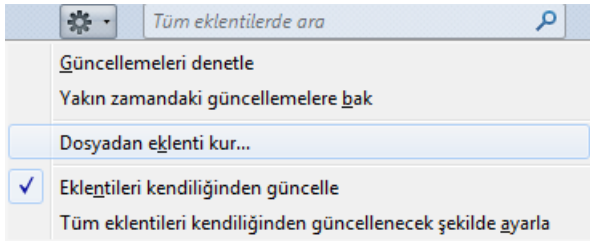
### 6.1 Thunderbird için TorBirdy Nasıl Kurulur?

[TorBirdy'yi bilgisayarınıza indirdikten](#) [163] sonra, **TorBirdy'yi** kurmaya aşağıdaki adımları takip ederek başlayın:

**1. Adım. Thunderbird'ü açın**, sonra 'ü **tıklayarak Thunderbird Menüsü'nü** görün ve **Eklentileri seçerek Eklentiler Yöneticisi** penceresini etkinleştirin.

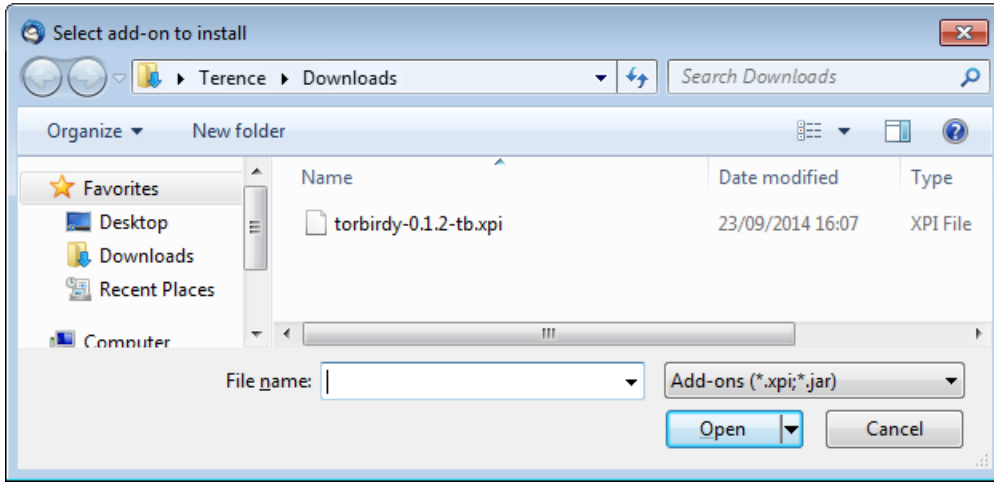
**2. Adım.** Sol yan çubuğundaki 'i **tıklayın**.

**3. Adım.** 'ı **tıklayıp** aşağıda görüldüğü gibi **Eklenti Dizinden Yükle'yi seçin**:



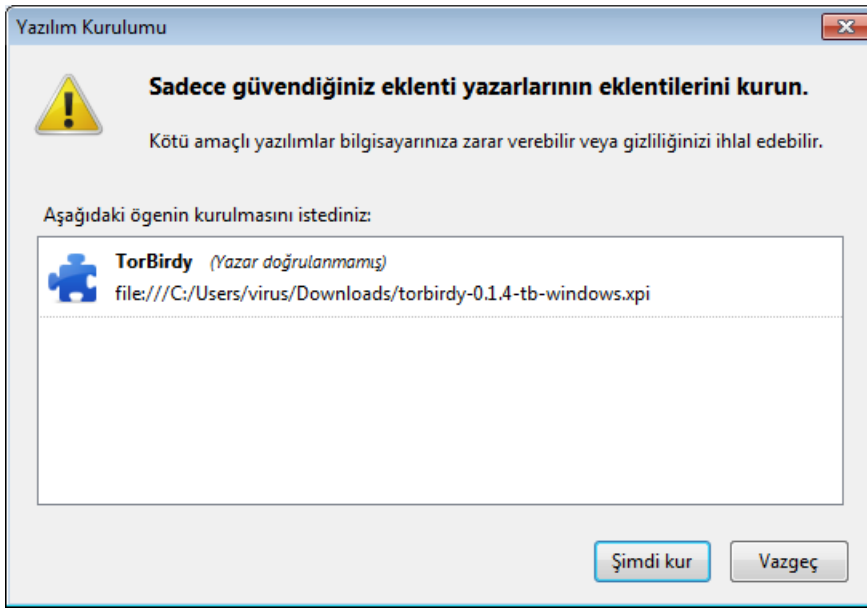
Şekil 1: Bütün Eklentiler için Araçlar menüsü

**4. Adım.** Aşağıdaki ekranda görüldüğü gibi TorBirdy eklentisini kaydettiğiniz dizine (büyük ihtimalle *İndirilenler* dizini) ilerleyin:



Şekil 2: Kululacak Eklentiye Seç ekranı

5. Adım: **Open** 'ı tıklayarak aşağıdaki ekranı etkinleştirin:



Şekil 3: Yazılım Kurulumu penceresi

**Önemli:** Bir sonraki adımı uygulamadan önce bütün e-postalarınız gönderilmiş ya da kaydedilmiş olduğundan emin olun!

6. Adım. **Şimdi kur** 'ı tıklayın ve sonra **Şimdi yeniden başlat (R)** 'ı tıklayarak Thunderbird programını yeniden çalıştırın ve **TorBirdy** eklentisinin kurulumunu tamamlayın.

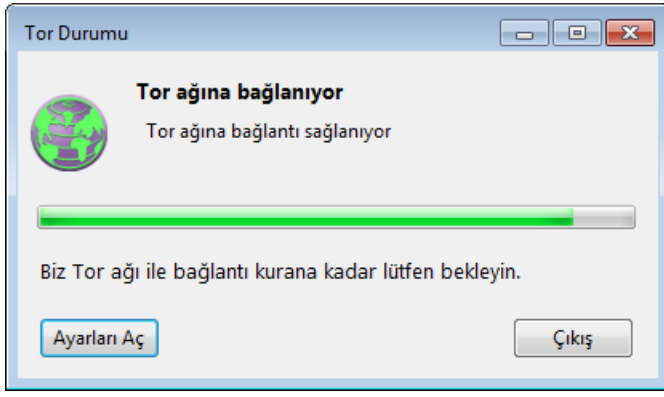
## 6.2 Thunderbird'de TorBirdy Nasıl Kullanılır?

Thunderbird ile TorBirdy'yi kullanabilmek için, önce **Tor Tarayıcı'nın** çalıştığından ve **Tor ağına** başarıyla bağlandığından emin olmalısınız. **Tor Tarayıcı'yı** henüz kurmadıysanız, lütfen devam etmeden önce **Tor Tarayıcı – Dijital Anonimlik ve Atlatma'ya** <sup>[193]</sup> bakınız.

### 6.2.1 Thunderbird için TorBirdy'yi Etkinleştirin

Aşağıdaki adımları takip ederek **Tor Tarayıcı'yı** başlatın ve Thunderbird'ü **Tor ağı** üzerinden çalıştırın

**Adım 1:** **Tor Tarayıcı** dizinine ilerleyin. **Start Tor Browser** 'e çift tıklayarak aşağıdaki ekranı etkinleştirin:



Şekil 8: Tor Statüsü penceresi

*Not: Tor Tarayıcı'nı başlatmadan önce açmış olduğunuz bütün Firefox pencerelerini kapatmanız önerilir*

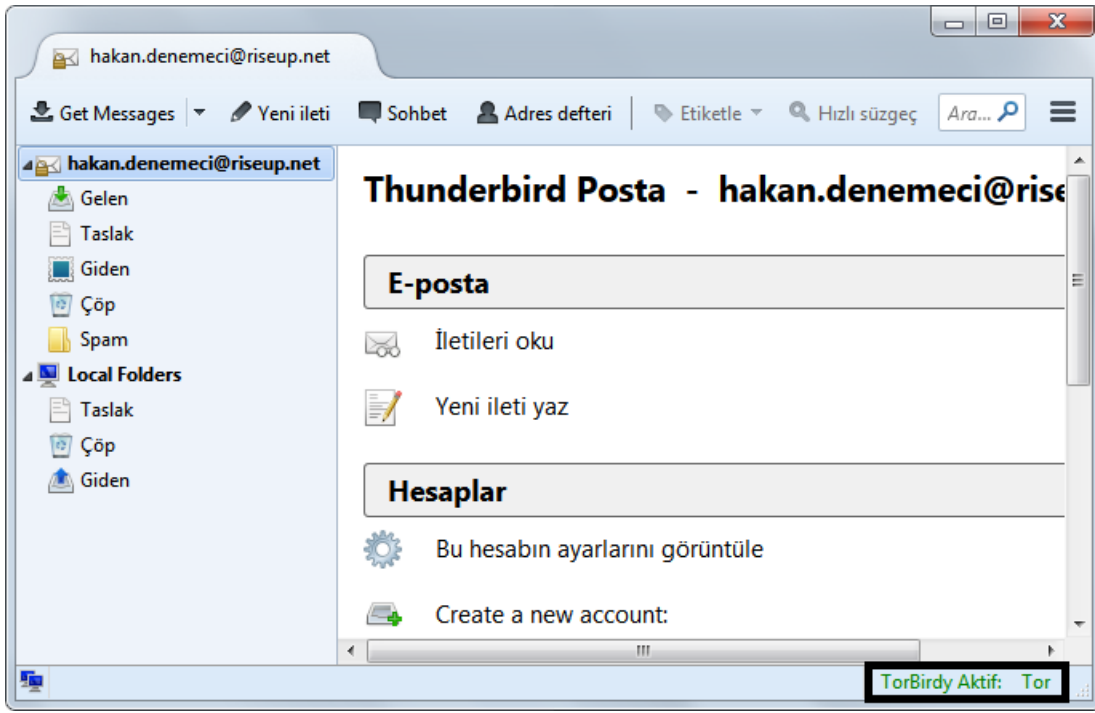
Bir müddet sonra, Tor Tarayıcı aşağıdaki gibi gösteren bir tarayıcı penceresi açacaktır:



Şekil 9: Tor Tarayıcı; Tor ağına başarıyla bağlanmış

Şimdi Tor ağına Tor tarayıcısıyla bağlısınız.

**2. Adım:** Thunderbird'ü **başlatın** ve sorulduğunda parolanızı girin. Aşağıdaki şekilde vurgulandığı gibi TorBirdy statüsü Thunderbird penceresinin sağ köşesinde gösterilecek:

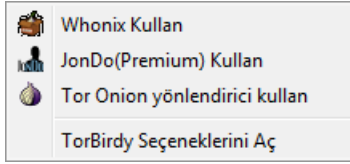


Şekil 10: Tor için Etkinleştirilmiş TorBirdy

## 6.2.2 TorBirdy'nin Tor'u kullanarak bağlandığını teyit edin

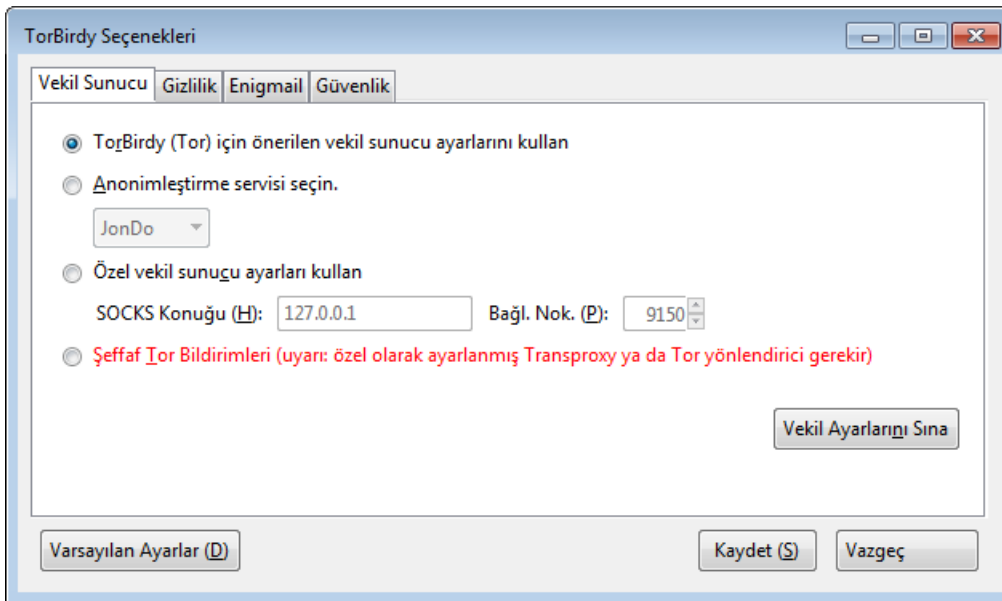
Aşağıdaki adımları takip ederek TorBirdy ayarlarını deneyin ve teyit edin

**1. Adım:** **TorBirdy Aktif: Tor** u tıklayarak aşağıdaki menüyü etkinleştirin



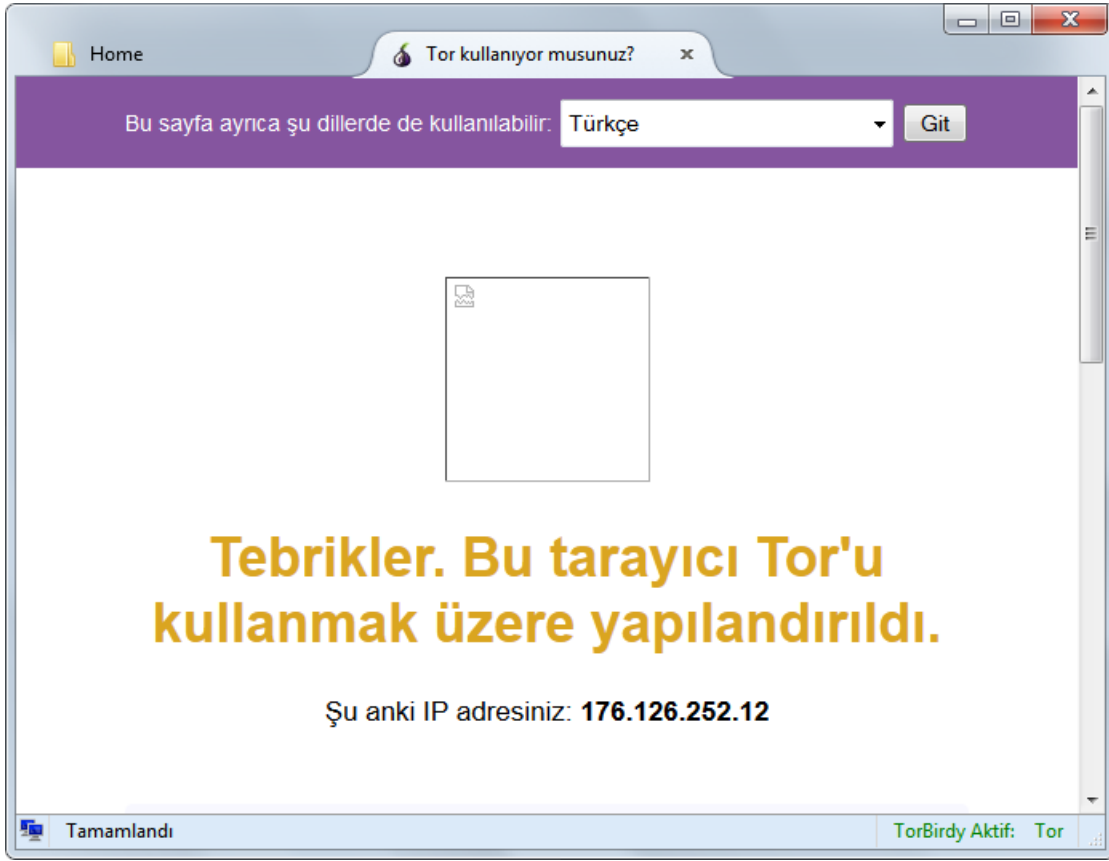
Şekil 11: Torbirdy Seçenekler Menüsü

**2. Adım:** Aşağıdaki pencereyi açmak için **TorBirdy Seçeneklerini Aç'ı seçin**. **TorBirdy Gelişmiş Seçenekleri** uyarı iletisinde **Tamam** ı tıklayın



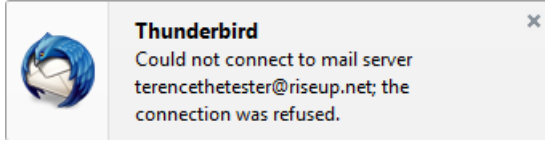
Şekil 12: TorBirdy Seçenekler penceresi

**3. Adım:** **Vekil Ayarlarını Sına** ı tıklayın. **Tor** ağı üzerinden başarı ile bağlandıysanız, aşağıdaki iletiyi göreceksiniz (\*IP adresleri değişecek):



Şekil 13: Tor'u Kullanıyor Musunuz? Penceresi

**Not:** Tor Tarayıcısı'nı başlatmamışsanız ya da Tor Tarayıcısı yukarıdaki 6.2.1 kısmında gösterildiği gibi Tor Ağı'na bağlanamıyorsa, e-posta sunucunuza bağlanamayacak ve muhtemelen Thunderbird'ü başlattığınızda şu iletiyi göreceksiniz:



Şekil 14: Bağlantı Reddedildi penceresi

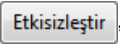
Not edilmelidir ki, Google Mail gibi bazı e-posta sağlayıcıları *Tor ağı* üstünden e-posta sunucularına bağlantıları geri çevirebilir.

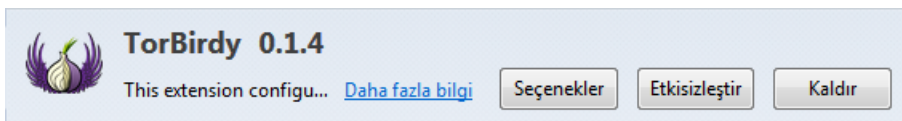
## 6.3 Thunderbird için TorBirdy'yi Etkisizleştirin

Thunderbird'ü TorBirdy'siz çalıştırmak isterseniz TorBirdy eklentisini aşağıdaki adımları takip ederek etkisizleştirebilirsiniz:

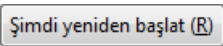
**1. Adım: Thunderbird'ü açın**, ve 'e tıklayarak *Thunderbird Menü'sünü* görüntüleyin. **Eklentileri seçerek Eklentiler Yöneticisi** penceresini etkinleştirin

**2. Adım:** Sol yan çubuğundaki 'i tıklayın

**3. Adım:** Aşağıdaki ekrandaki 'i tıklayın:



Şekil 15: TorBirdy Eklentisi'ni Etkisizleştir

**4. Adım:** 'ı tıklayarak Thunderbird'ü yeniden açın ve TorBirdy'yi etkisizleştirmiş olun.

# Sıkça Sorulan Sorular ve Gözden Geçirme

## 7. Sıkça Sorulan Sorular

**Soru:** Sadece Enigmail'i kurup GnuPG'yi kurmazsam ne olur?

**Cevap:** Enigmail çalışmaz. Nihayetinde, **GnuPG Enigmail'in** kullandığı şifreleme motorunu sağlayan yazılımdır.

**Soru:** Thunderbird'de kaç tane e-posta hesabı kurabilirim?

**Cevap:** Dilediğiniz kadar! **Thunderbird** 20 ya da daha fazla e-posta hesabının altından rahatlıkla kalkabilecek bir e-posta yazılım programıdır!

**Soru:** Bir arkadaşımın Riseup ve Gmail hesaplari var. Onu Thunderbird, Enigmail ve GnuPG kullanması için ikna etmeli miyim?

**Cevap:** En iyisi bu tabii ki. Sadece emin olun ki bütün güvenlik ayarlarını tamamen sizin gibi yapılandırsın. Böylelikle birbirinizle gizlilik ve güvenlik içinde çok etkin bir şekilde iletişim kurabileceksiniz.

**Soru:** Bir kere daha tekrarlayabilir misiniz, Enigmail bir e-posta iletinin hangi bölümlerini şifreler?

**Cevap:** Enigmail mesaj içeriğini şifreler. İletinin konu satırını, senin e-posta adresini ya da e-posta adresinle ilişkilendirmeyi tercih ettiğiniz ismi şifrelemez. Bu yüzden gizli bir mesaj yollamak istiyorsanız, konu satırının sizi ele vermemesine dikkat edin! Ve anonim kalmak istiyorsanız, gerçek adınızı göstermemeye ya da e-posta hesabı yaratırken gerçek adınızı kullanmamaya özen gösterin.

**Soru:** Hala iletilerimi dijital olarak imzalamamın amacını anlamış değilim.

**Cevap:** ADijital bir imza bir iletinin gerçek yollayıcısının sen olduğunu ve iletinin amaçlanan alıcıya giden yolunda oynanmamış olduğunu kanıtlar. Onun çok önemli bir mektup içeren zarfın üzerindeki tuğranın elektronik eşdeğeri olduğunu düşünebilirsiniz.

## Firefox ve eklentileri - Güvenli Web Tarayıcısı

### Short Description:

**Mozilla Firefox** ücretsiz ve gittikçe daha sık kullanılır hale gelen bir web tarayıcısıdır. Mozilla Firefox'un kapsamı kendisi için geliştirilen, web'de dolaşırken gizlilik ve güvenliğinizi korumak için tasarlanmış olanlar dahil, çok sayıda eklenti sayesinde geliştirilmiştir.

### Online Installation Instructions:

#### Firefox'u indirme

- Kısa **Uygulamalı Rehberler'in** <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Firefox** ikonunu **tıklayarak** <https://www.mozilla.org/tr/firefox/new/> sayfasını açın
- Kurucuyu kaydetmek için **Ücretsiz İndir** bağlantısını **tıklayın** ve kurucuyu **bulup** üzerine **çift tıklayın**
- Rehberi takip edin ve 4. ve 5. kısımlara geldiğiniz zaman **NoScript** ve diğer eklentileri **kurun**
- **Firefox tarayıcınıza eklenti kurmak için - Firefox'u başlatın** - Aşağıdaki ikonların üzerine **tıklayın** ve daha sonra karşınıza çıkan sayfada **Firefox'a ekle** düğmesine basın
- Kurulum tamamlandıktan sonra, bilgisayarınıza kaydetmiş olduğunuz kurucu ve eklentileri silebilirsiniz.

### Firefox: NoScript: Adblock Plus: Better Privacy: Beef Taco: HTTPS Everywhere:



### Ana Sayfa

- <https://www.mozilla.org/tr/firefox/new/> <sup>[194]</sup>

### Bilgisayar Gereksinimleri

- Tüm Windows Sürümleri

### Bu Rehberde Kullanılan Sürüm

- Firefox 24.0
- NoScript 2.6.8.1
- HTTPS Everywhere 3.4.1

- Adblock Plus 2.3
- Better Privacy 1.68
- Beef Taco 1.3.7

#### Bu bölümün son güncellenme tarihi

- Eylül 2013

#### Lisans

- Ücretsiz ve Açık kaynak yazılım

**Seviye:** 1: Giriş, 2: Basit, 3: Orta Derece, 4: Deneyimli, 5: Gelişmiş

**Bu araçları kullanmaya başlamak için gereken zaman:** 20-30 dakika

#### Buradan sağlayacağınız faydalar:

- Özellikleri çok sayıda eklenti sayesinde geliştirilebilen sağlam ve güvenli bir internet tarayıcısı
- Potansiyel olarak tehlikeli program ve kötücül web sitelerinden kendinizi koruma yetisi
- Bilgisayardan tüm tarama izlerinizi silme yetisi

#### GNU Linux, Mac OS ve Microsoft Windows ile çalışan diğer programlar:

**Mozilla Firefox** tarayıcı **GNU Linux, Mac OS, Microsoft Windows** ve diğer işletim sistemleri için ulaşılabilir. Web sayfaları kötücül yazılımların en temel kaynağı olduğu için onların güvenli kullanımı *hayati önemdedir*. Bu yüzden, **Mozilla Firefox** ve tavsiye edilen eklentileri kullanmanızı şiddetle tavsiye ederiz. **Firefox'un** ücretsiz ve açık kaynak çapraz platform bir program olarak sunduğu güvenlik avantajları, **Internet Explorer** gibi daha ticari olan eş değer programlara göre çok daha fazladır. Yine de, **Mozilla Firefox'tan** başka bir program kullanmayı tercih ederseniz, **GNU Linux, Mac OS** ve **Microsoft Windows** ile çalışabilen aşağıdaki alternatifleri öneririz:

- [Google Chrome](#) [200]
- [Opera](#) [201]

## 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

Bu bölüm herhangi bir web tarayıcısı kullanmayı bildiğinizi varsayar, bu yüzden de **Mozilla Firefox'un** tarama özelliklerinin nasıl kullanılacağını açıklamaz. Buradaki amaç **Mozilla Firefox'u** daha güvenli kullanmak için gereken ek özellikler hakkında bilgi vermektir.

- **Mozilla Firefox Eklentileri**, **Firefox'un** var olan özelliklerini geliştiren veya ona yeni özellikler ekleyen küçük programlardır.
- **Mozilla Firefox Plugins** genellikle üçüncü taraflarca yazılımlarının Firefox tarayıcısında kullanılabilmesi üzere tasarlanmış küçük çaplı yazılımlardır.

Bu bölüm, **Firefox** web tarayıcısının ve tüm İnternet deneyiminizin daha gizli ve güvenli hale gelmesini sağlamak için **Mozilla Eklentilerini** nasıl indirip, kurup kullanabileceğinizi açıklar.

**NoScript** eklentisi **4.0 NoScript Hakkında** [202] bölümünde ayrıca incelenmiştir. Diğer eklentiler **Diğer Faydalı Firefox Eklentileri** [183] kısmında incelenmiştir.

**Önemli:** Kötücül yazılım ve casus yazılımların büyük bir çoğunluğu web sayfalarından gelir. Bu yüzden de, özellikle e-posta yoluyla gönderilen web adreslerini açmanın güvenli olup olmadığı konusunda her zaman çok dikkatli olmalısınız. Herhangi bir sayfayı açmadan önce web adresini aşağıdaki sayfa tarayıcılarını kullanarak taramanızı tavsiye ederiz:

- [www.virustotal.com](http://www.virustotal.com) [203]
- [www.onlinelinkscan.com](http://www.onlinelinkscan.com) [204]
- [www.phishtank.com](http://www.phishtank.com) [205]

Web sitelerinin güvenilirliği ile ilgili bilgileri aşağıdaki tarayıcıları kullanarak da edinebilirsiniz:

- <http://safeweb.norton.com> [206]
- [www.urlvoid.com](http://www.urlvoid.com) [207]

#### Offline Installation Instructions :

**\*\*Firefox Kurulumu\***

- Kısa **Uygulamalı Rehberler'in** [1] Giriş bölümünü okuyun
- Aşağıdaki **Firefox** ikonunu **tıklayın** ve yükleyiciyi 'Aç'ın veya 'Çalıştır'ın. Gerekirse yükleyiciyi önce kaydedin, daha sonra üzerine çift tıklayın
- Devam etmeden önce bir sonraki bölümdeki 'Kurulum yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulum gerçekleştirildikten sonra silebilirsiniz



[208]



[209]



[210]

[211]

[212]

[213]

# Firefox Nasıl Kurulur ve Yapılandırılır?

Bu sayfadaki kısımların listesi:

- [2.0 Firefox Hakkında](#)
- [2.1 Firefox Nasıl Kurulur?](#)
- [2.2 Genel bölme seçenekleri nasıl yapılandırılır?](#)
- [2.3 Gizlilik bölmesi seçenekleri nasıl yapılandırılır?](#)
- [2.4 Güvenlik bölmesi seçenekleri nasıl yapılandırılır?](#)
- [2.5 Gelişmiş bölme seçenekleri nasıl yapılandırılır?](#)

## 2.0 Firefox Hakkında

**Firefox'un** İnternet erişiminizi daha gizli ve güvenli hale getirecek kullanımı kolay birçok özelliği vardır. bu ayarları hangi sıklıkta yapılandırmanız gerektiği durumunuza göre değişir::

- Kişisel bilgisayarınızı kullanıyorsanız ve başka kişilerin bilgisayarınızı kullanmasına izin vermiyorsanız bu ayarları bir kere yapılandırmanız yeterlidir.
- Kamusal bir alanda veya işteyseniz, kendi kullanımınız için bu ayarları düzenli olarak yeniden yapılandırmanız gerekebilir.

**Not:** İsterseniz USB bellek çubuğuna koyabileceğiniz, taşınabilir bir **Firefox** versiyonu kullanabilirsiniz. Böyle yaparsanız **Firefox'u** gereksinimlerinize göre yapılandırabilir ve herhangi bir kamusal bilgisayarda kullanabilirsiniz. Taşınabilir **Firefox** ile ilgili daha fazla bilgi için [Mozilla Firefox, Taşınabilir Sürüm](#) [214] bölümüne bakınız.

## 2.1 Firefox Nasıl Kurulur?

**Firefox'u** kurmak basit bir işlemdir. **Firefox'u** kurmaya başlamak için aşağıdaki adımları takip edin:

**1. Adım.**  **Firefox Setup Stub 36.0.1** 'nin üzerine **çift tıklayın**, **Klasör Aç – Güvenlik Uyarısı** kutusu görünürse paketten çıkarma ilerleme çubuğunu görmek üzere için 'Çalıştır'ı **tıklayın**.

*Bir süre sonra, Firefox Kurulum Sihirbazına Hoş geldiniz penceresi belirecek.*

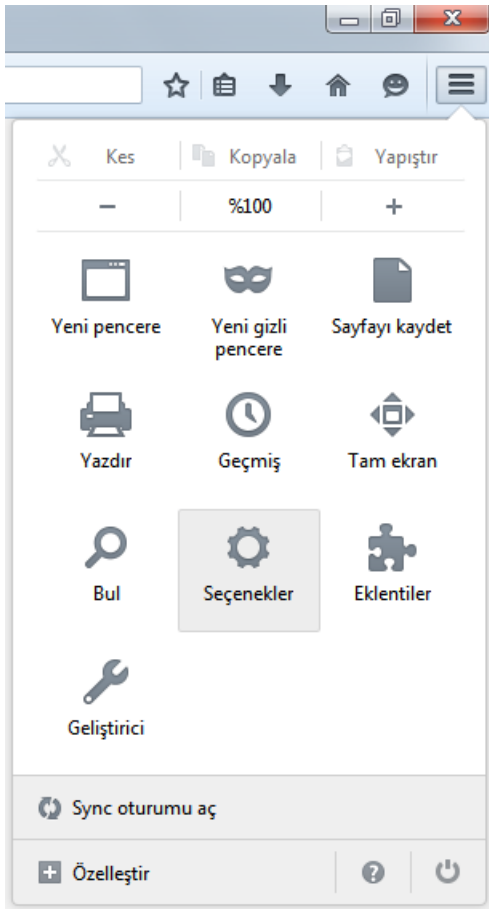
**2.Adım.** Kurulum işlemleri kılavuzundaki adımları **takip edin** ve verili seçenek ve ayarları kabul edin.

**Not:** Belirli bir sebebiniz yoksa verili seçenek ve ayarları değiştirmeyin.

## 2.2 Genel bölme seçenekleri nasıl yapılandırılır?

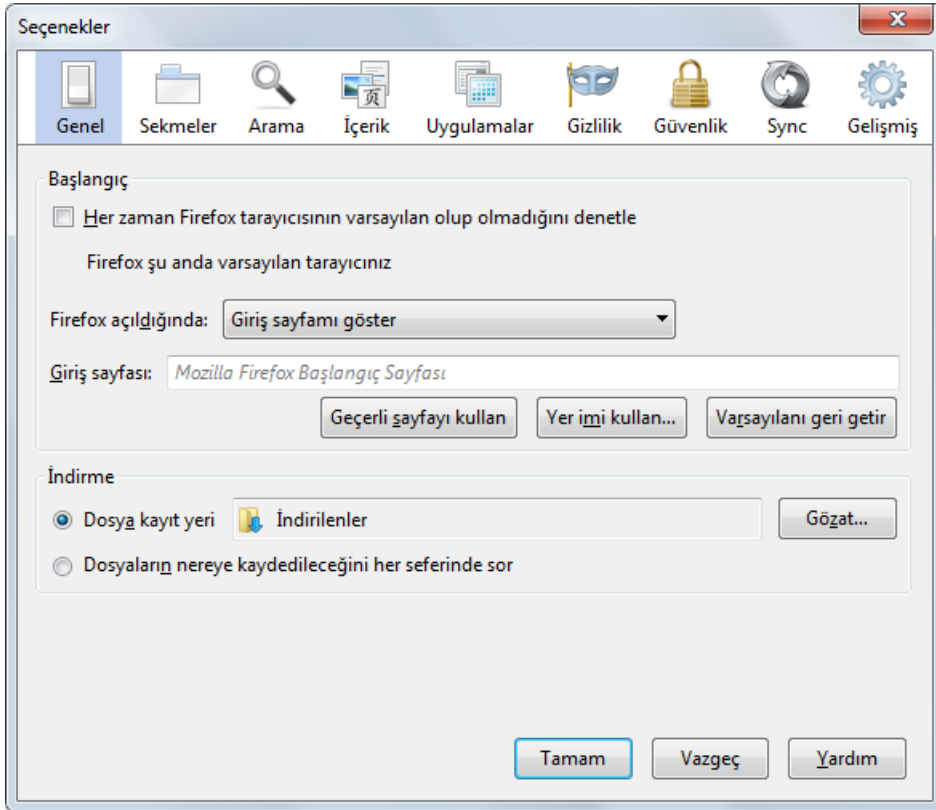
**Firefox'u** yapılandırmak için aşağıdaki adımları takip edin:

**1.Adım.** **Firefox** menü sekmesinden **Seçenekler'i** aşağıda görüldüğü gibi **seçin**:



Şekil 1: Seenekler seili Aralar menüsü

Bunu yaptığınız zaman Seenekler penceresi aşağıda görüldüğü gibi etkinleşecektir:



Şekil 2: Verili Genel bölmeyi gösteren Seenekler penceresi

**Tavsiye:** Genel bölme yukarıda Şekil 2'de görüldüğü gibi otomatik olarak açılmazsa 'i tıklayın.

Genel bölmesi, bir iki temel **Firefox** ayarlarını yapılandırmanıza yardımcı olacaktır. Bunların arasında tercih ettiğiniz ana

sayfa ve *İndirilenler* dosyasının konumu gibi özellikler vardır.

Firefox başlayınca adlı aşağı açılan menüdeki verili ayar *Ana sayfamı göster* şeklindedir ve verili ana sayfanız *Mozilla Firefox Başlangıç Sayfası*'dir.

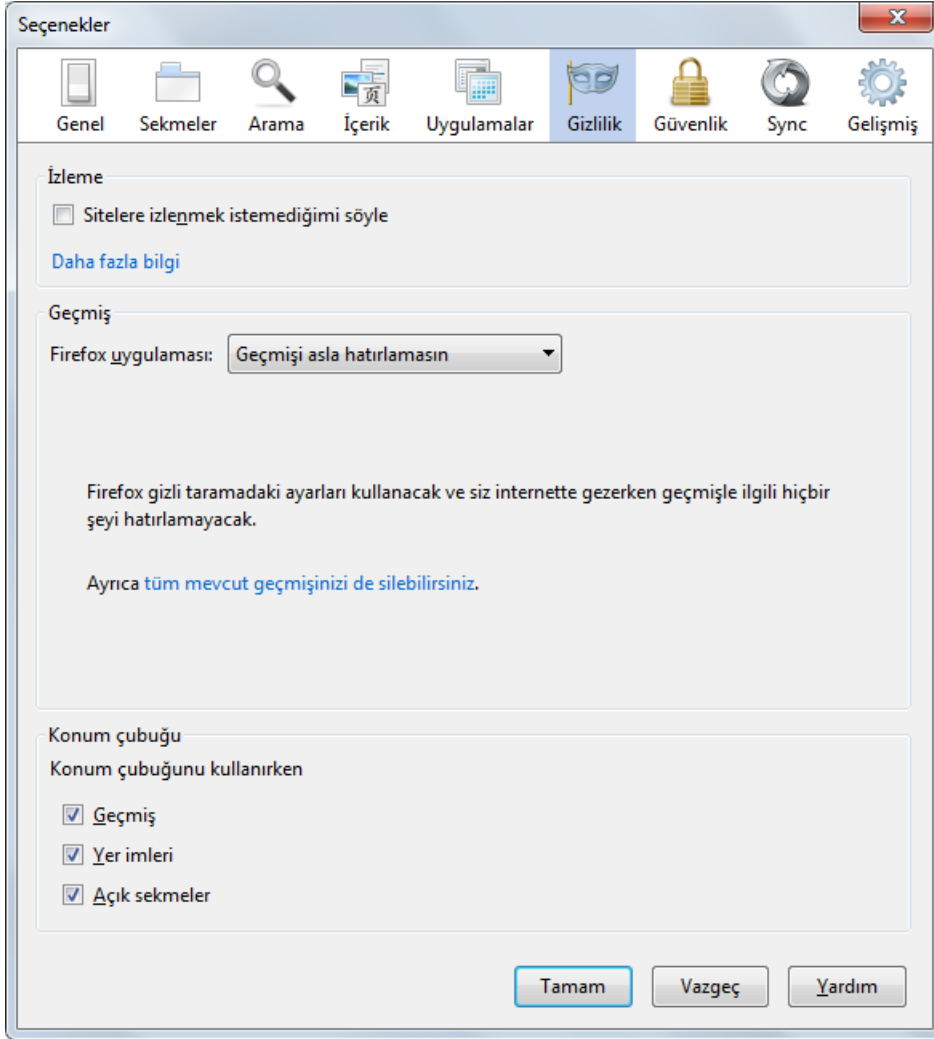
**Tavsiye:** Güvenilir bulduğunuz başka bir sayfayı ana sayfanız olarak belirlemek için [Geçerli sayfayı kullan](#) ı tıklayın.

## 2.3 Gizlilik bölmesi seçenekleri nasıl yapılandırılır?

*Gizlilik* bölmesi tarayıcınızın gizlilik ve güvenlik ayarlarını yapmanızı sağlar.



**1. Adım.** Aşağıda görünen ekranı etkinleştirmek için [Gizlilik](#) 'i tıklayın.



Şekil 3: *Gizlilik* bölmesini gösteren Seçenekler penceresi

*Gizlilik* bölmesi üç kısma ayrılmıştır: İzleme bölümü, Geçmiş bölümü ve Konum çubuğu bölümü.

- **İzleme Bölümü**

*İzlemeyi durdur* adlı bölümde, internet etkinlik ve eylemlerinizin, örneğin reklam şirketleri, analitik araştırmalar veya piyasa araştırmacıları gibi üçüncü taraflarca denetlenip izlenmesi hakkındaki tercihlerinizi yapabilirsiniz. Firefox'u ilk kurduğunuz zaman, verili ayar *Tercihlerim hakkında siteye bilgi verme* olarak belirlenmiştir ve değiştirilmesi gerekir. Bunu *İzlenmek istemiyorum* olarak değiştirmeniz, şirket ve organizasyonların izlenmek istemediğiniz hakkında bilgilendirilmesini sağlayacaktır.

**Not:** *İzlemeyi durdur* seçeneği güven sistemine dayanır ve gönüllüdür. Bu yüzden de web siteleri hukuki ve teknik olarak bu tür isteklere uymak zorunda değildir. Bu isteğe saygı duyan organizasyonların sayısı gün geçtikçe artsa da, *İzlemeyi durdur* seçeneği, doğrudan ticari ve zararlı çıkarları hedef alan eklentiler ile desteklenmelidir. Bunu yapmak, potansiyel olarak zararlı çevrim içi reklamlara maruz kalma riskinizi azaltır. **Firefox** eklentileri ile ilgili daha fazla bilgi edinmek için, **Diğer Faydalı Firefox Eklentileri** <sup>[183]</sup> bölümüne bakabilirsiniz.

İzleme

☒ Sitelere izlenmek istemediğimi söyle

[Daha fazla bilgi](#)

Şekil 4: İzleme bölümü

**1. Adım.** *Sitelere izlenmek istemediğimi söyle* seçeneğini (yukarıdaki Şekil 4'te görüldüğü gibi) **işaretleyin** ve katılımcıların gizlilik ve güvenliğinize saygı duymasını sağlayın.

- **Geçmiş Bölümü**

Geçmiş bölümü, **Firefox** tarayıcınızın 'geçmiş'i ile ilgili ayarlarını yapmanızı sağlar. Bu tarih, **Firefox** kullanmaya başladığınız andan itibaren ziyaret ettiğiniz sitelerin listesini içerir. Verili seçenek *Firefox Geçmişini hatırlasın* olacaktır ve internet gizliliği ve güvenliğinizi için değiştirilmelidir.

Tarama geçmişinizin izlerini silmek için aşağıdaki adımları takip ediniz:

**1. Adım.** *Firefox* aşağı açılır menüsünü **etkinleştirin** ve *Geçmişini asla hatırlamasın* seçeneğini Şekil 3'te görüldüğü gibi **seçin**.

**2. Adım.** Aşağıdaki ekranı etkinleştirmek için [tüm mevcut geçmişinizi de silebilirsiniz.](#) 'i **tıklayın**:

Tüm geçmişini sil

Temizlenecek zaman aralığı: Her şey

 Tüm geçmiş silinecek.  
Bu işlem geri alınamaz.

Ayrıntılar

- ☒ Tarama ve indirme geçmişi
- ☐ Form ve arama geçmişi
- ☒ Çerezler
- ☒ Önbellek
- ☒ Etkin oturumlar
- ☒ Çevrim dışı site verileri
- ☒ Site tercihleri

[Şimdi temizle](#) [Vazgeç](#)

Şekil 5: Tüm tarihi sil penceresi

**3. Adım.** Tüm kutucukları **işaretleyin** ve [Şimdi temizle](#) 'yi tıklayarak **Firefox'un** potansiyel olarak bilgilerinizi içeren verilerden temizleyin. Şimdi *Gizlilik* bölümüne dönebilirsiniz.

- **Konum çubuğu bölümü**

*Konum çubuğu* bölümü işaretlenmiş olan web sitelerinden adres, çerezler ve benzeri geçici verileri kullanır ve tarama kolaylığınız için **Firefox Evrensel Kaynak Konumlayıcı (Universal Resource Locator, URL)** çubuğunda adres önerisinde bulunmak için web tarihinizden faydalanır. *Konum çubuğunu kullanırken* kısmındaki verili seçenek *Geçmiş ve Yer imlerinden öneride bulun*'dur ve internet gizliliğinizi ve güvenliğinizi korumak için değiştirilmelidir.

Tarama alışkanlıklarınız ve geçmişinizin izlerini silmek için aşağıdaki adımları takip ediniz:

**1. Adım.** *Konum çubuğunu kullanırken*, aşağıda Şekil 6'da görüldüğü gibi öneri kaynakları ile ilgili bütün işaretleri **kaldırın**.

Konum çubuğu

Konum çubuğunu kullanırken

- ☐ Geçmiş
- ☐ Yer imleri
- ☐ Açık sekmeler

Şekil 6: Öneri kaynakları ile ilgili bütün seçeneklerin kaldırıldığı Konum Çubuğu bölümü

2. Adım. Ayarlarınızı teyit etmek ve **Seçenekler** penceresinden çıkmak için **Tamam** butonunu tıklayın.

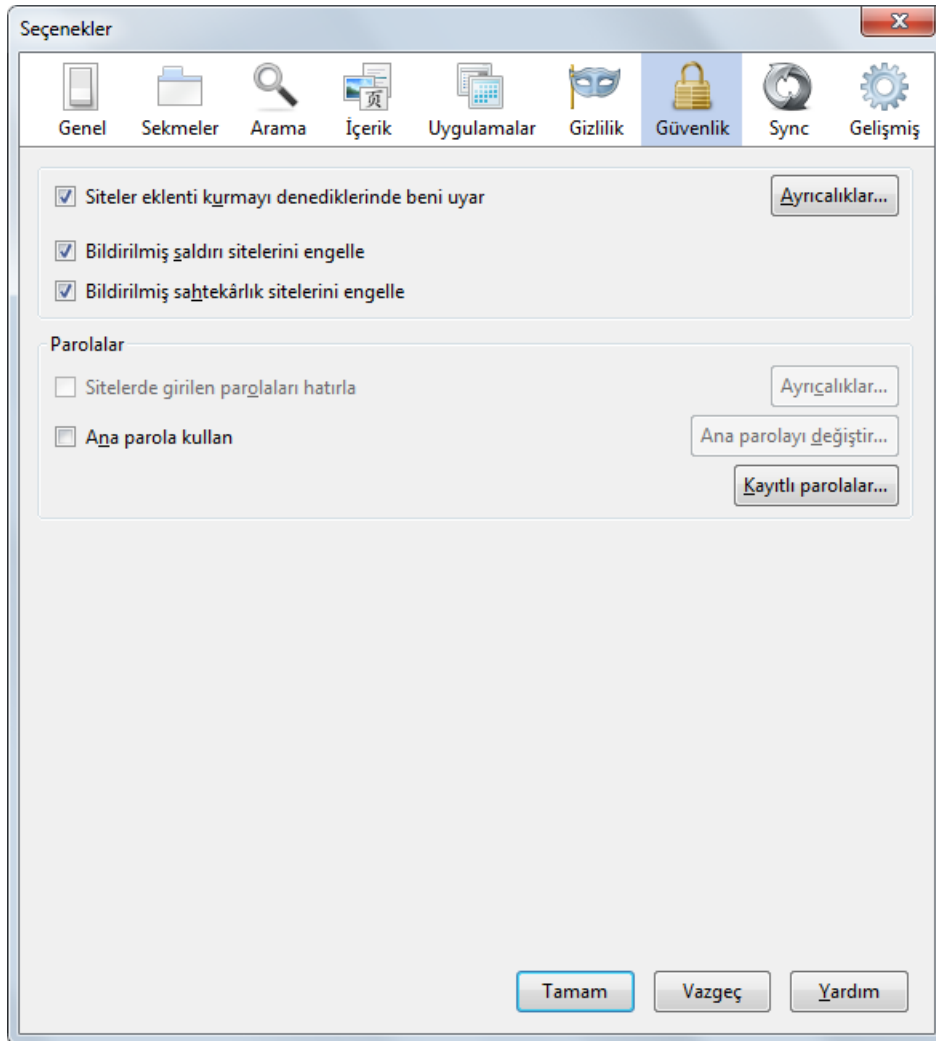
**Not:** Geçici verilerinizi daha güvenli ve ayrıntılı bir şekilde silmek istiyorsanız, **CCleaner** [65] ile ilgili bölüme bakabilirsiniz.

## 2.4 Güvenlik bölümü seçenekleri nasıl yapılandırılır?

**Güvenlik** bölümü iki kısma ayrılmıştır: birinci kısım, dış kaynaklardan gelecek potansiyel olarak tehdit edici eylemlerle ilgilenirken, ikinci kısım, ya da **Parola** kısmı, parola ile ilgili ayarlar yapmanızı sağlar.

**Not:** Parola saklama ile ilgili daha fazla bilgi için lütfen **KeePass** [215] bölümüne bakınız.

1. Adım. **Seçenekler** penceresini etkinleştirmek için **Firefox** menü çubuğundan **Araçlar > Seçenekler**'i seçin. Aşağıda görünen ekranı etkinleştirmek için **Güvenlik** sekmesini tıklayın.



Şekil 7: Güvenlik bölümünü gösteren Seçenekler penceresi

2. Adım. Birinci kısımdaki verili ayarları **kabul edin**.

- **Parola kısmı**

**Parolalar** kısmı parolalarınızla ilgili ayarları yapmanızı sağlar. **Firefox**'u ilk defa kurup çalıştırdığınız zaman **Siteler için parolaları hatırla** seçeneği verili olarak işaretlidir ve gizlilik ve güvenliğiniz için devre dışı bırakılmalıdır. Parolalarınızı güvenli bir şekilde **KeePass**'te [215] saklamanızı tavsiye ederiz.

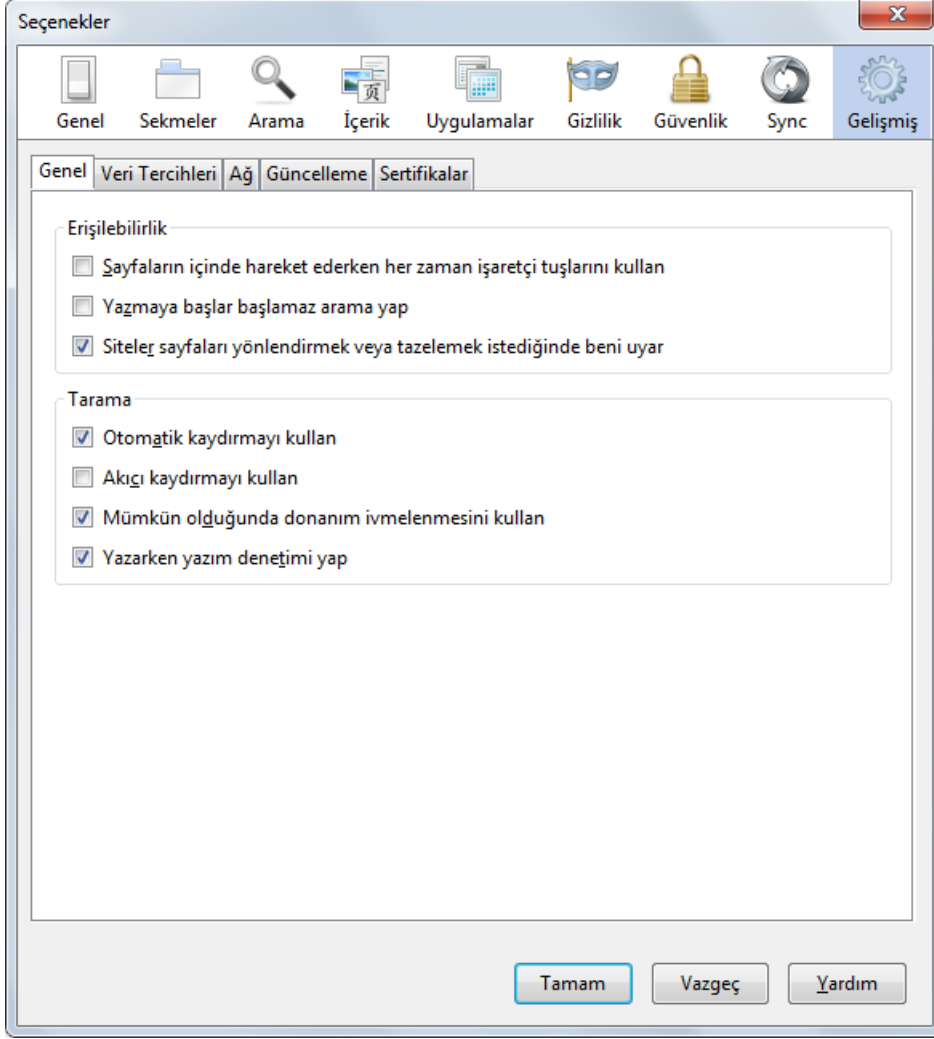
3. Adım. **Seçenekler** penceresinde **Güvenlik** bölümünü yapılandırmayı tamamlamak için **Tamam** butonunu tıklayın.

## 2.5 Gelişmiş Bölmesi Seçenekleri Nasıl Yapılandırılır?

**Gelişmiş** sekmesi, isminin de gösterdiği gibi, **Deneyimli Firefox** kullanıcıları için tasarlanmıştır. Fakat, **Genel** sekmesinde aşağıda bahsedeceğimiz seçeneği kullanıma sokmak **her** seviyedeki kullanıcı için fayda sağlayacaktır.

- **Web siteleri sayfayı yönlendirmek veya yeniden yüklemek istediği zaman beni uyar** seçeneği **Firefox**'un web sitelerinin otomatik olarak sizi başka bir sayfaya yönlendirmesini veya sizin bilginiz veya onayınız olmadan yeniden

yüklemesini engeller.



Şekil 8: Verili Genel sekme seçili halde Gelişmiş bölümü

**1. Adım.** Web siteleri sayfayı yönlendirmek veya yeniden yüklemek istediği zaman beni uyar seçeneğini yukarıdaki Şekil 8'de görüldüğü gibi **etkinleştirin**.

**2. Adım.** Değişiklikleri uygulamak için **Tamam** butonuna tıklayın ve Gelişmiş sekmesinden çıkın.

Tebrikler! Artık **Firefox** ile interneti gizli ve güvenli bir şekilde kullanabilirsiniz.

## Firefox Eklentileri Nasıl Kurulur?

Bu sayfadaki bölümlerin listesi:

- **3.0 Mozilla Eklentileri Hakkında**
- **3.1 Mozilla Eklentileri Nasıl Kurulur?**
- **3.2 Mozilla Eklentisi Nasıl Devre Dışı Bırakılır veya Silinir?**
- **3.3 Mozilla Eklentileri Nasıl Güncellenir?**
- **3.4 Mozilla Yan Uygulamaları Nasıl Güncellenir?**

## Mozilla Eklentileri Hakkında

**Mozilla** ürünleri bağlamında eklentiler, yeni özellikler ekleyen veya var olan işlevleri genişleten hafif yazılımlardır. Bu yüzden, bazen *uzantı* olarak da adlandırılırlar. Örneğin, **NoScript** eklentisi, **Firefox'un** tanımlanmış sunuculardan gelen kodları bloke etme özelliğinin kapsamını genişletir.

**Eklenti** genel olarak, üçüncü taraflar tarafından yazılımlarının **Firefox** tarayıcısı içinde kullanılabilmesi için tasarlanmış yazılım parçalarıdır. Yaygın olarak kullanılan eklentilere bir örnek olarak **Adobe Flash** içeriğini **Firefox** tarayıcısı penceresinde görüntülemeye yarayan **Flash** eklentisini verebiliriz.

### 3.1 Mozilla Eklentileri Nasıl Kurulur?

**Mozilla eklentilerini** indirmek ve kurmak kolay ve basittir. Farklı eklentileri indirmek ve kurmak için aşağıdaki adımları takip edin:

**1. Adım. Başla > Mozilla Firefox'u seçin** ve **Firefox'u** açmak için masa üstündeki **Firefox** ikonuna **çift tıklayın**.

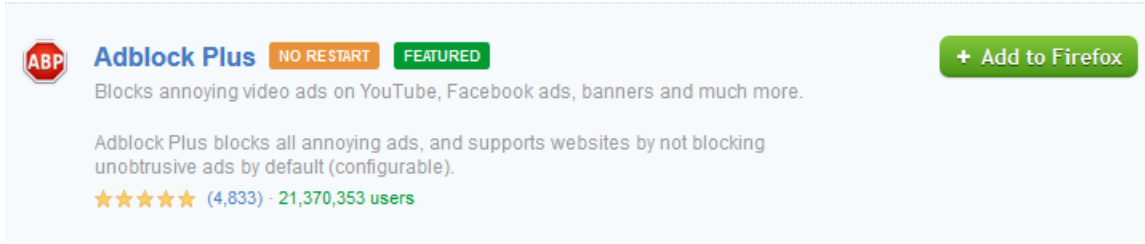
**2. Adım. Firefox** adres çubuğuna <https://addons.mozilla.org/> <sup>[216]</sup> **yazın** ve **Enter'a basın**. Bu şekilde **Firefox için Mozilla Eklentilerisitesi** etkinleşecektir.

**3. Adım. Mozilla** arama bölümüne aşağıda görüldüğü gibi eklentinin ismini **yazın** (bu örnekte **AdblockPlus** eklentisi kullanılmıştır):



Şekil 1: Adblock Plus gösteren Mozilla Firefox eklenti arama çubuğu

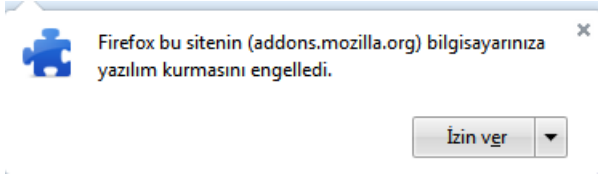
**4. Adım.**  u ya da **tıklayarak** ya da **Enter'a** basarak aşağıdaki ekranı açın:



Şekil 2: Adblock Plus bölümü için Arama Sonuçları

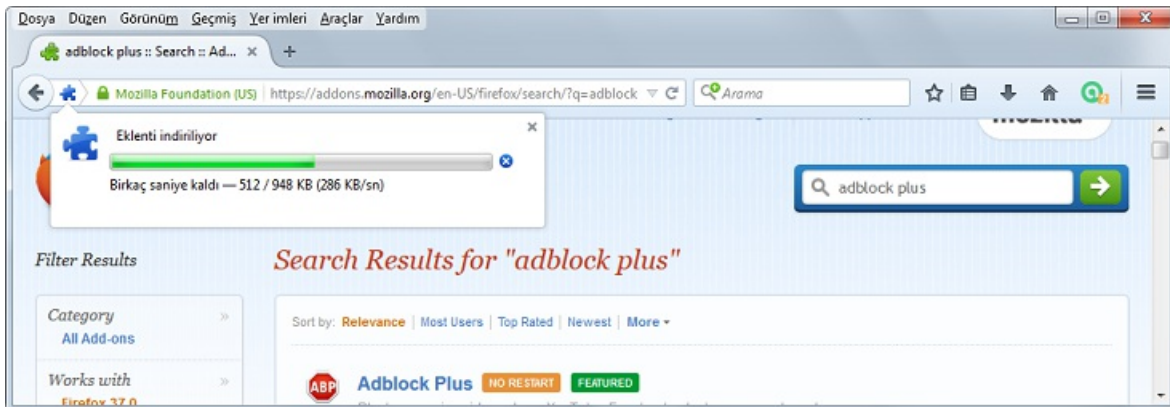
**Tavsiye:** Yeşil renki **Firefox'a Ekle** düğmesi, ancak imleç belli bir eklentinin üstüne gelince görünür.

**5. Adım.** Aşağıdaki ekranları etkinleştirmek için  u **tıklayın**.

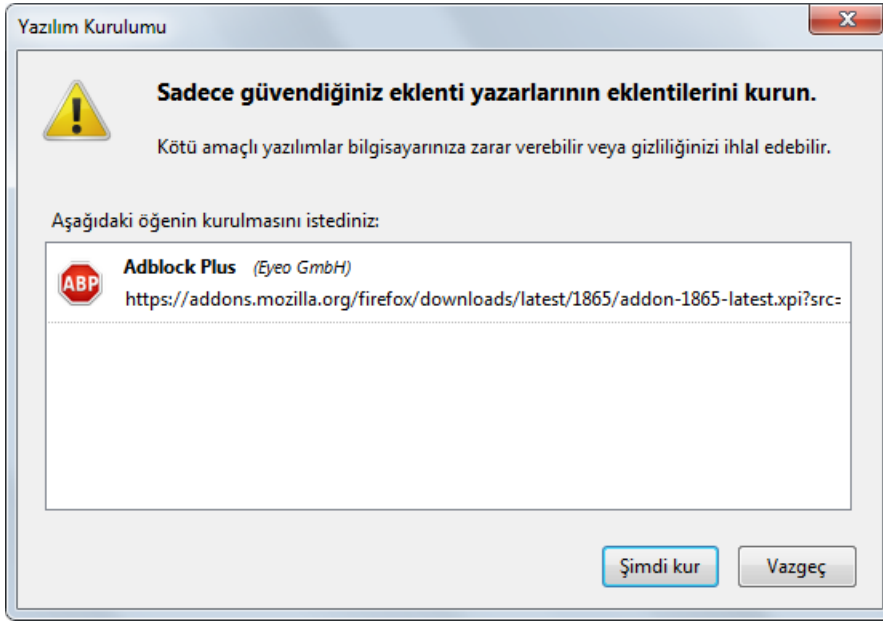


Şekil 3: Adblock Plus :: Ara :: Firefox Eklentileri – Mozilla Firefox penceresi

**6. Adım.** Aşağıdaki pencereleri etkinleştirmek için  i **tıklayın**:

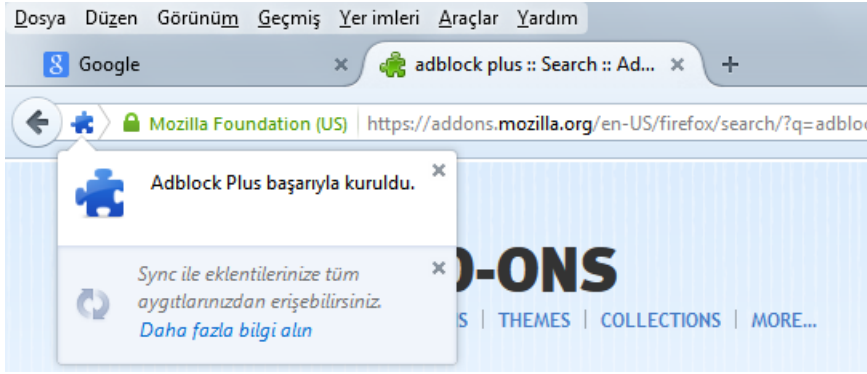


Şekil 4: The Adblock Plus :: Ara :: Mozilla Firefox için Eklentiler



Şekil 5: Adblock Plus Yazılım penceresi

**7. Adım.** Kullanıma soktuktan sonra **Şimdi kur** butonunu tıklayın ve eklentiyi kurmaya başlayın. Kurulum tamamlandıktan sonra aşağıdaki pencereyi göreceksiniz:

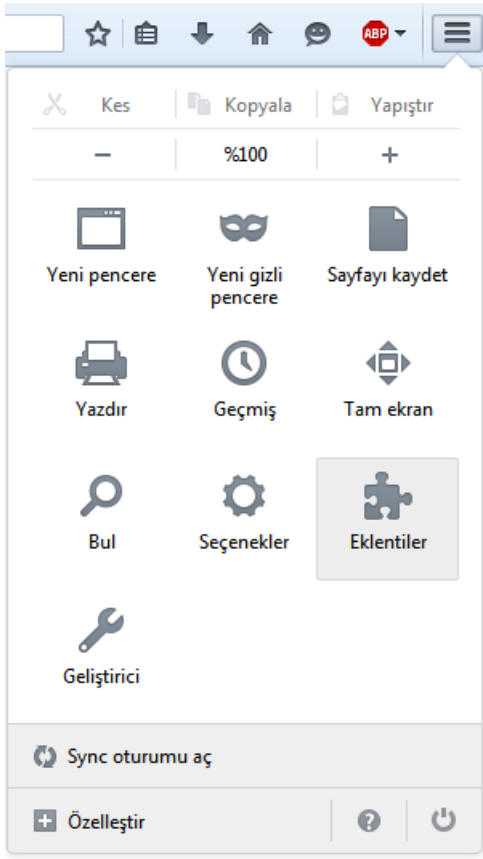


Şekil 6: Adblock Plus :: Ara :: Firefox Eklentileri – Mozilla Firefox ve açılan ileti

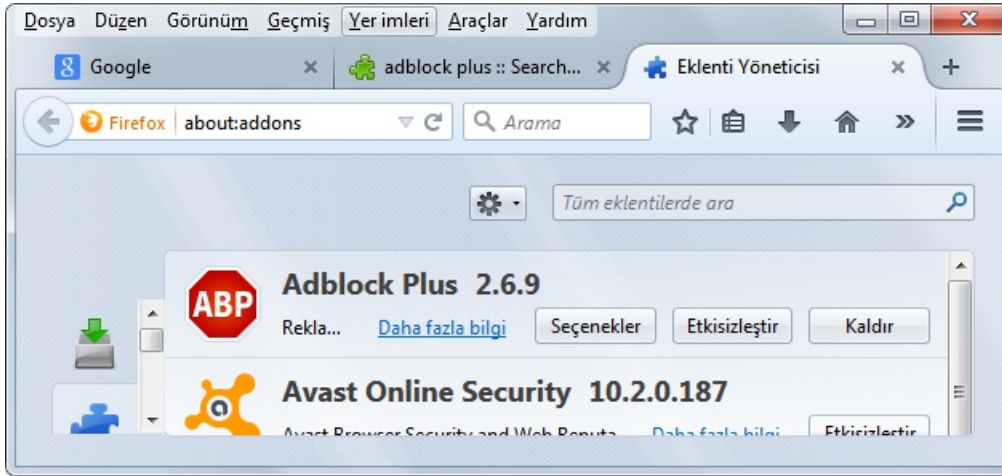
**Tavsiye:** Birçok eklenti ve uzantının başarılı bir şekilde kurulması için **Firefox'un** yeniden başlatılması gerekir.

**Şimdi yeniden başlat** butonunu veya **Yeniden başlat** butonunu tıklayın ve **Firefox'u** hemen yeniden başlatmak istemiyorsanız **Daha Sonra** seçeneğini seçin.

**8. Adım.** Firefox menü sekmesindeki **Araçlar** menüsünden **Eklentiler'i** seçin ve aşağıdaki ekranı etkinleştirin:



Şekil 7: Eklenti seçeneği seçilmiş Araçlar menüsü



Şekil 8: Yeni kurulmuş Adblock Plus eklentisini gösteren Eklentileri Düzenle sekmesi

**Önemli:** Bilmediğiniz kaynaklardan eklenti kurmayın. Bunu yerine, eklentileri her zaman daha güvenli olan <https://addons.mozilla.org/> [216] web sitesinden edinin.

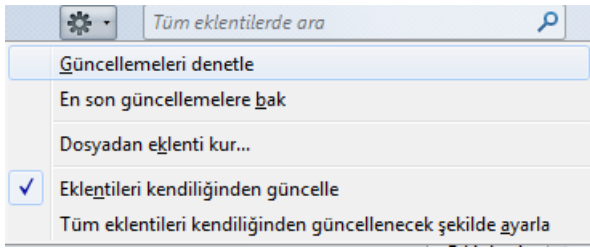
### 3.2 Mozilla Eklentisi Nasıl Devre Dışı Bırakılır veya Silinir?

*Eklentiler* sekmesi, kurulmuş olan tüm eklentileri Şekil 8'deki gibi gösterir. Herhangi bir **Mozilla** eklentisini geçici olarak devre dışı bırakmak için **Etkisizleştir** butonunu **tıklayabilir** veya tamamen silmek için **Kaldır** butonunu **tıklayabilirsiniz**. Fakat bazı durumlarda bu değişikliklerin uygulanabilmesi için **Firefox'u** yeniden başlatmak gerekebilir.

### 3.3 Mozilla Eklentileri Nasıl Güncellenir?

Eklentilerin, **Firefox'un** en son versiyonu ile uyumlu çalışabilmesi için sıklıkla güncellenmeleri gerekir. Bağlantınızın hızına bağlı olarak bağlantıları otomatik veya manuel olarak güncellemeyi tercih edebilirsiniz.

**1. Adım.** İlgili aşağı açılır menüyü etkinleştirmek için **Etkisizleştir** butonunu **tıklayın** ve **Güncellemeleri kontrol et'i seçin**. Bu sayede eklentilerinizi aşağıdaki Şekil 9'da görüldüğü gibi manuel olarak güncelleyebilirsiniz.



Şekil 9: İlgiliolan aşağı açılır menüyü gösteren Eklenti Düzenleyici güncelleme düğmesi

**2. Adım.** Ya da, *Eklentileri Otomatik Olarak Güncelle*'yi **seçerek** eklentilerinizi yukarıdaki Şekil 9'da görüldüğü gibi otomatik olarak güncelleyebilirsiniz.

### 3.4 Mozilla Yan Uygulamaları Nasıl Güncellenir?

Bazı yan uygulamaların otomatik olarak güncellenemediğini göz önünde bulundurursak, kullanıcıların **Mozilla Yan Uygulamalarının** güncellemelerini manuel olarak kontrol etmelerini şiddetle tavsiye ederiz. .

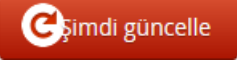
Güncellemeleri manuel olarak kontrol etmek için aşağıdaki adımları takip ediniz:

**1. Adım.** Aşağıdaki siteyi etkinleştirmek için <https://www.mozilla.com/plugincheck> [217] adresine **tıklayın**:



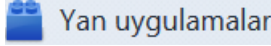
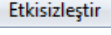
Şekil 10: Mozilla Firefox Yan Uygulama Kontrol ve Güncelleme sitesi

**2. Adım.** Sitede sunulan farklı yan uygulama sorunlarını aşağıdaki farklı düğmeler yoluyla **kategorize edebilirsiniz**:

-  ibaresini gösteren yan uygulamaları bu düğmeye *anında* basarak güncellenenizi **şiddetle** tavsiye ederiz. Bastıktan sonra size sunulan adımları takip edebilirsiniz. (Bu düğme listesini bitirdikten sonra kullanımda olmayan yan uygulamaları devre dışı bırakabilir ya da silebilirsiniz.)
-  ibaresini gösteren yan uygulamaları, gerekli olmadıkları ya da tek tek güncellenmedikleri takdirde devre dışı bırakabilir veya silebilirsiniz.
-  ibaresini gösteren yan uygulamaları tek tek gözden geçirin ve hangisinin gerekli olduğuna karar verin. Bilinmeyen veya gerekli olmayanları devre dışı bırakabilir veya silebilirsiniz.

Bilinmeyen veya artık gerekli olmayan yan uygulamaları **devre dışı bırakmak** için aşağıdaki adımları takip ediniz:

**1. Adım.** **Araçlar >Eklentiler**'i seçin ve *Eklenti Düzenleyici* sekmesini etkinleştirin.

**2. Adım. Mozilla Firefox** yan uygulamalarının tümünü görüntülemek için  **tıklayın** ve devre dışı bırakmak istediğiniz eklentiyi seçin, ardından  **tıklayın**.

Bir yan uygulamayı **bilgisayarınızdan silmek** istiyorsanız:

**1. Adım. Başlat > Kontrol Paneli'ni seçin.**

**2. Adım.** **Program kaldır veya değiştir**, **tıklayın**.

**3. Adım.** Pencereden ilgili olan programı seçin ve **kaldır**'u **tıklayın**.

*Yan Uygulama Kontrol ve Güncelleme* sayfasındaki tüm sorunlar çözülene kadar bu işlemleri tekrar edin. Minimum ayda bir olmak üzere güncellemeleri kontrol etmeniz **çok önemlidir**. Yan uygulamalar, güvenlik problemlerini çözmek üzere düzenli olarak geliştirilir ve güncellenirler.

**ÖNEMLİ: Adobe Flash ve Oracle Java** birçok güvenlik açığı içerir ve bilgisayarınızın kontrolünün uzaktaki kişilerin eline geçmesine yol açabilir ve bilgi ve verilerinize erişim sağlayabilecek virüsleri bilgisayarınıza kurabilirler. Bu yüzden, bu programları bilgisayarınızdan silmeniz veya en azından **Firefox** bağlantılı eklentilerini devre dışı bırakmanızı **şiddetle** tavsiye ederiz. Java'nin nasıl devre dışı bırakılacağı veya silineceği hakkında daha fazla bilgi edinmek için, [Java'yı bilgisayarınızdaki tüm tarayıcılardan nasıl silebilirsiniz?](#) <sup>[218]</sup> veya [Java'yi bilgisayarınızdan nasıl kaldırabilirsiniz?](#) <sup>[219]</sup> sayfalarına bakabilirsiniz.

## NoScript Eklentisi Nasıl Kullanılır?

Bu sayfadaki kısımların listesi:

- **4.0 NoScript Hakkında**
- **4.1 NoScript Nasıl Kullanılır?**

### 4.0 NoScript Hakkında



**NoScript**, bilgisayarınızı İnternet'teki zararlı web sitelerinden korumaya yarayan bir **Mozilla eklentisidir**. Sizin kabul ettiğiniz, güvenilir bulduğunuz web sitelerinin (banka sayfası veya çevrim içi gazete gibi) 'beyaz listesi'ni yaparak çalışır. Geriye kalan tüm siteler, siz içeriklerinin zararlı olmadığını kanıtlayana kadar, potansiyel olarak zararlı tehlikeli kabul edilir. Güvenilir olduğuna karar verdiğiniz siteleri beyaz listeye ekleyebilirsiniz.

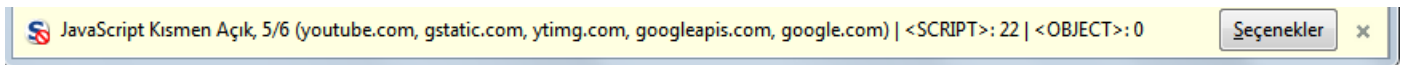
**NoScript** tüm reklam bantları ve açılır reklamları, **JavaScript** ve **Java** kodlarını ve diğer potansiyel olarak tehlikeli web site özelliklerini otomatik olarak engeller. **NoScript** zararlı içerik ile bir web sitesini göstermek için gerekli olan içeriği birbirinden ayırt edemez. Bu yüzden de, içeriğinin güvenilir olduğuna inandığınız siteler için istisnalar yapılmasını sağlamak size kalmıştır.

### 4.1 NoScript Nasıl Kullanılır?

**NoScript** kullanmaya başlamadan önce, **Araçlar > Eklentiler'i seçerek Eklentiler** penceresini etkinleştirin ve **NoScript'in** başarılı bir şekilde kurulduğundan emin olun.

**Tavsiye: NoScript'in** kullanımı en başta zor görünse de (çünkü düzenli olarak ziyaret ettiğiniz web sitelerinin içerikleri düzgün görünmemeye başlayabilir), otomatik engelleme özelliğinin faydasını görmeye hemen başlayacaksınız. Bu sayede, rahatsız edici reklamlardan, açılır mesajlardan ve web sitelerine eklenmiş zararlı kodlardan korunabilirsiniz.

**NoScript, JavaScript, Adobe Flash** ve diğer kod benzeri içerikleri yakalayana kadar arka planda sessiz bir şekilde çalışır. Yakaladığı zaman, bu içeriği engelleyecektir ve **Firefox** penceresinin altında aşağıdaki statü çubuğunu çıkaracaktır:



Şekil 1: NoScript statü çubuğu

**NoScript** statü çubuğu, hangi *nesnelerin* (örneğin reklam ve açılır mesajları) ve *kodların* kendilerini bilgisayarınıza yerleştirmekten alıkoymadığını gösterir. Aşağıda görünen iki şekil **NoScript'in** nasıl çalıştığını başarılı bir şekilde gösterir: **Şekil 2'de NoScript'in** ticari bir web sitesinde **Adobe Flash Player** tarafından oynatılan bir reklamı nasıl engellediğini görebilirsiniz.



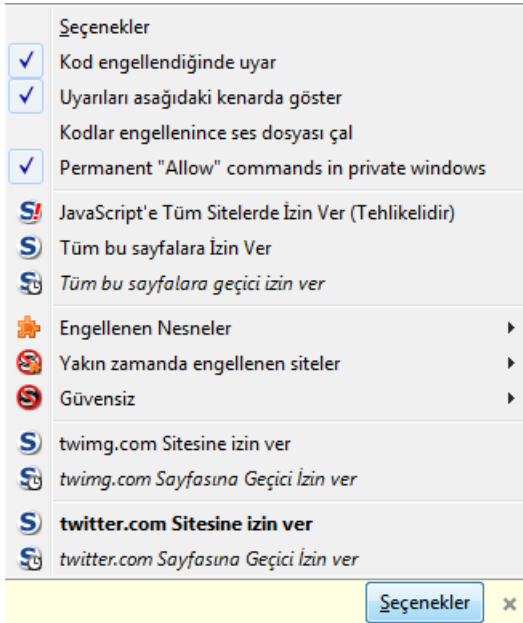
Şekil 2: NoScript'in ticari bir sitedeki açılır bir reklamı engelleme örneği

Şekil 3'te, **Twitter** web sitesinin, kendisini görüntüleyebilmek için **JavaScript'in** (en azından geçici olarak) etkinleştirilmesi gerektiği iletisini verdiğini görebilirsiniz.



Şekil 3: Twitter web sitesinden gelen JavaScript'in etkinleştirilmesi isteği

**NoScript** zararlı ve gerçek kodları birbirinden ayırt edemediği için, bazı önemli özellikler ve işlevler (örneğin bir araç çubuğu) görünmez hale gelebilir. Bazı web siteleri birden fazla web sitesinden gelen içerik veya kod benzeri içerik gösteriyor olabilir. Örneğin, **www.twitter.com** web sitesinin iki kod kaynağı vardır (*twitter.com* ve *twimg.com*):



Şekil 4: NoScript statü barı Seçenekler menüsü örneği

Bu şartlar altında, kodları engellemek için, *[web sitesi ismi]'e Geçici Olarak İzin Ver* seçeneğini **seçebilirsiniz** (bu örnekte, *twitter.com'a Geçici Olarak İzin Ver*). Bu sayfayı görmeniz için yeterli olmazsa deneme yanılma yöntemi ile seçtiğiniz içeriğin görüntülenmesi için minimum kaç web sitesine ihtiyaç olduğunu belirleyebilirsiniz. **Twitter** örneğinde, **Twitter'ın** düzgün çalışabilmesi için, **twitter.com'a Geçici Olarak İzin Ver** ve **twimg.com'a Geçici Olarak İzin Ver'i** seçmelisiniz.

**Uyarı! Hiçbir** şart altında, *Kodlara Her Zaman İzin Ver (tehlikeli)* seçeneğini seçmemelisiniz. Mümkün oldukça, *Bu Sayfadaki Tüm Bilgilere İzin Ver* seçeneğini de işaretlememelisiniz. Bazı durumlarda tüm kodlara izin verme seçeneğini işaretlemeniz gerekebilir. Bu durumlarda, bu işlemi gerçekten güvendiğiniz siteler için, geçici olarak ve çevrim içi işlemleriniz bitene kadar yaptığınızdan emin olun. Tehlikeli kodların çevrim içi gizliliğinizi ve güvenliğinizi tehdit eder konuma gelmesi için *bir an* bile yeterlidir.

Güvendiğiniz ve düzenli olarak ziyaret ettiğiniz web siteleri için, (web sitesinin ismi)'ne **İzin Ver'i seçin**. (Yukarıdaki örnekte *twitter.com'a İzin Ver* ve *twimg.com'a İzin Ver* seçilmişti.) Bu seçeneği işaretleyerek **NoScript'in** bu web sitesini kalıcı olarak güvenilir web siteleri listesine eklemesini sağlayabilirsiniz.

## Diğer Faydalı Firefox Eklentileri

Bu sayfadaki bölümlerin listesi:

- **5.0 Eklentiler Hakkında**
- **5.1 HTTPS Everywhere Nasıl Kullanılır?**
- **5.2 Adblock Plus Nasıl Kullanılır?**
- **5.3 Beef Taco (Hedeflenen Reklam Çerezleri Önerileri) Nasıl Kullanılır?**
- **5.4 Better Privacy Nasıl Kullanılır?**
- **5.5 Diğer Faydalı Eklentiler**

### 5.0 Eklentiler Hakkında

Bu bölümde bahsedilen **Mozilla Firefox uzantıları**, tarayıcı ile yaptığınız işlemlerdeki anonimlik, gizlilik ve güvenliği geliştirmek için tasarlanmıştır. Bu eklentileri indirmek için, lütfen **Firefox'u indirme** <sup>[86]</sup> bölümüne bakınız.

### 5.1 HTTPS Everywhere Nasıl Kullanılır?



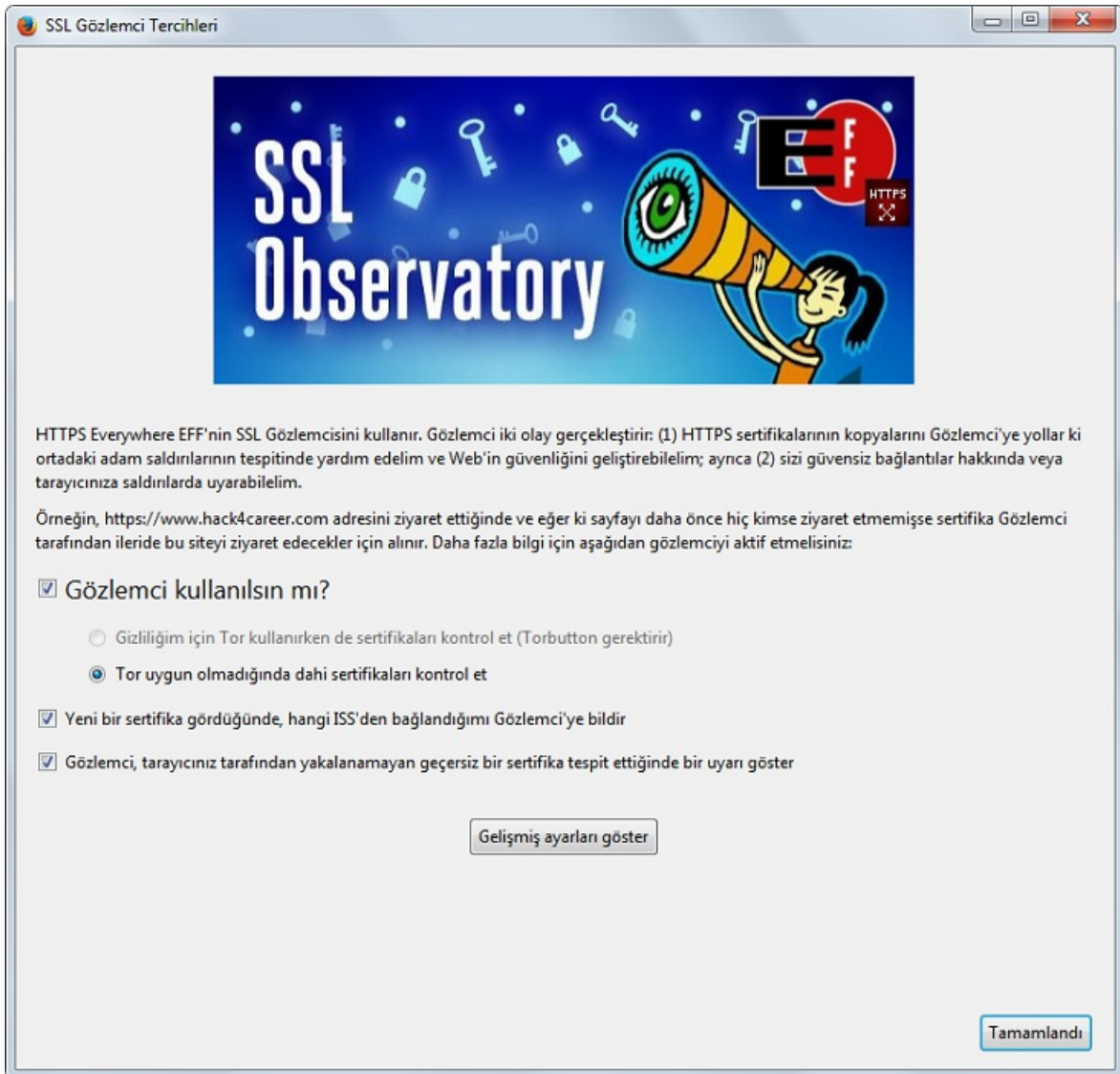
**HTTPS Everywhere** belirlenen web siteleri ile her zaman şifrelenmiş (https) bir kanal üzerinden iletişim kurmanızı sağlayan bir **Mozilla Firefox** uzantısıdır. Bazı siteler şifreleme imkanı sunsa da, birçoğu şifrelenmemiş bir http adresi üzerinden iletişim kurma eğilimi taşır. **HTTPS Everywhere** eklentisi, bu siteleri **HTTPS** protokolü üzerinden yeniden yazarak bu problemleri çözer. Seçilen bu web siteleri ile bağlantınızın güvenli olması için arka planda sessiz bir biçimde çalışır. Fakat, ancak bu sitelerin kendileri **HTTPS** protokolü kullanıyorsa çalışır.

**HTTPS Everywhere** eklentisinin kurulumunu başarılı bir şekilde tamamladıktan sonra aşağıdaki ekranı göreceksiniz:



Şekil 1: HTTPS Everywhere SSL Observatory kullanmalı mı? uyarı ekranı

**1. Adım:** Aşağıdaki ekranı etkinleştirmek için 'i tıklayın:



Şekil 2: SSL Observatory Tercihler ekranı

**Not:** Firefox tarayıcınıza daha önce **HTTPS Everywhere** kurduysanız, **Araçlar > HTTPS Everywhere > SSL Observatory Tercihler'i seçin** ve **Observatory Kullan** ve **Yeni bir lisans görüldüğü zaman, hangi ISP'den bağlandığımı Observatory'ye bildir** seçeneklerinin işaretli olmasına dikkat edin. **Tor** kullanmıyorsanız, **Tor'a erişim olmasa da Lisansları Kontrol Et** seçeneğinin **işaretli** olduğundan emin olun.

## Adblock Plus Nasıl Kullanılır?



**Adblock Plus**, reklamların görünmesini engelleyen veya kısıtlayan bir içerik süzme uzantısıdır.

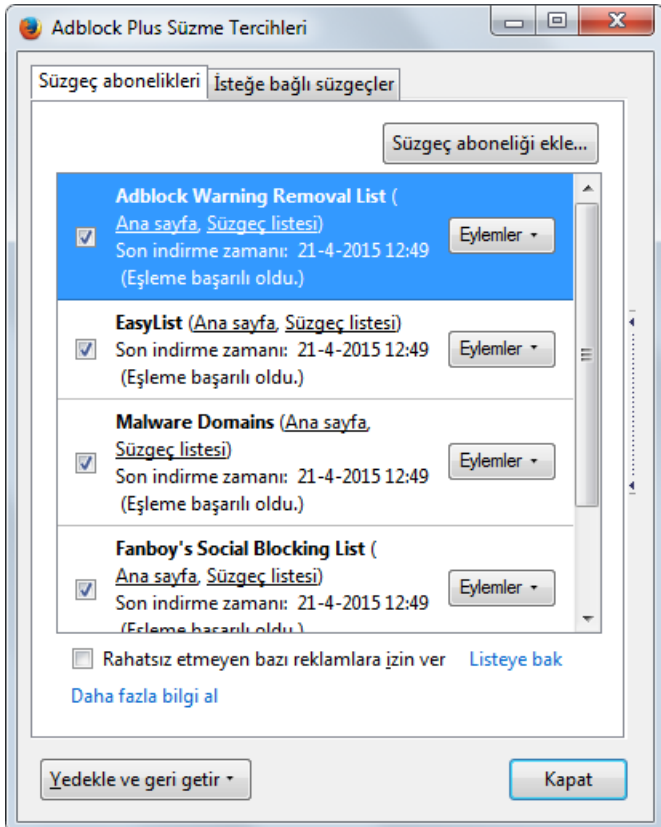
**Adblock Plus** başarılı bir şekilde kurulduktan sonra, aşağıdaki sayfa başlatılacaktır:  
<chrome://adblockplus/content/ui/firstRun.html> <sup>[220]</sup>



Şekil 3: Adblock Plus krom içerik sayfası

**1. Adım.** Zararlı İçerik Engelleme, Sosyal Medya Düğmelerini Kaldır ve İzlemeyi Engelle seçeneklerini (yukarıda Şekil 1'in gösterdiği gibi) etkinleştirmek için ☐ KAPALI ibaresini ☒ AÇIK haline **getirin**.

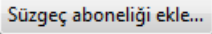
**2. Adım.** Aşağıda görünen ekranı etkinleştirmek için **Araçlar > Adblock Plus > Süzgeç tercihleri...**'ni seçin4:

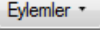


#### Şekil 4: Üç süzgeç aboneliği gösteren Adblock Plus Süzgeç Tercihleri

**3. Adım.** Her abonelik kutusunu tek tek **işaretleyin** (yukarıda Şekil 2'de görüldüğü gibi) ve

☐ Rahatsız etmeyen bazı reklamlara izin ver seçeneğini **devre dışı bırakın**. Bu şekilde bu süzgeçlerde listelenmiş olan tüm reklamlar filtrelenecektir.

**4. Adım.** Birden fazla dil kullanıyorsanız, 'yi **tıklayın** ve farklı süzgeç aboneliklerini görün. Daha sonra, abonelikler açılır listesini etkinleştirmek için 'i **tıklayın** ve uygun olanı **seçerek** 'yi **tıklayın**.

**4. Adım.** Süzgeç aboneliklerinizi güncellemek için 'i **tıklayın** ve açılır menüden *Süzgeçleri Güncelle*'yi **seçin**.

### 5.3 5.3 Beef Taco (Hedefli Reklam Çerezlerini Önleme) Nasıl Kullanılır?



**Beef Taco**, içinde **Google**, **Microsoft** ve **Yahoo'nun** da olduğu çeşitli şirketlerin reklamları ile bağlantılı çerezleri düzenlemenizi sağlayan bir **Mozilla Firefox** eklentisidir. Hedeflenen Reklam Çerezleri Önerileri olarak bilinen çerezleri otomatik olarak devre dışı bırakacak şekilde yapılandırılabilir. Daha **Deneyimli** ve **Gelişmiş** kullanıcıların, hangi çerezlerin sistemde kalması ve hangilerinin devre dışı bırakılmasına detaylı bir şekilde karar vermelerine de olanak sağlar.

### 5.4 Better Privacy Nasıl Kullanılır?



**Better Privacy**, bilgisayarınıza **Flash** kodu tarafından yerleştirilebilen ve LSO (Local Shared Objects) olarak bilinen özel çerezlerden korunmanıza yardımcı olan bir **Mozilla Firefox** eklentisidir. Bu çerezler, **Firefox'un** standart çerez temizleme yöntemleri tarafından temizlenemezler.

### 5.5 Diğer Faydalı Eklentiler

Bu bölümde, web'i daha gizli ve güvenli bir şekilde taramanıza yardımcı olacak, ücretsiz ve açık kaynak (veya açık kaynak olma sürecinde olan) birkaç faydalı eklentiyi bulabilirsiniz.

#### 5.5.1 Cryptocat



[221]

**Cryptocat** tarayıcınızda çalışan, açık kaynak, şifreli ve güvenli bir Anlık Mesajlaşma eklentisidir. Bazı durumlarda, diğer yazılı mesaj yazılımlarına göre, kullanması daha kolaydır. **Cryptocat**, tüm üyelerle veya katılımcılarla bire bir mesajlaşabileceğiniz sanal bir mesajlaşma odası yaratır. Tüm mesajlar, gönderilmeden ve alınmadan önce kişinin tarayıcısında şifrelenmiş hale getirilir. **Cryptocat**, **Mozilla Firefox**, **Google Chrome**, **Apple Safari** ve **Mac OS X** app için tarayıcı eklentisi olarak bulunmaktadır. Daha fazla bilgi için, [burayı tıklayın](#). [222]

#### 5.5.2 Disconnect



[223]

**Disconnect** verilerinizi üçüncü taraflardan korumak ve izleyenleri analiz ederek, reklamcılar, analizciler ve sosyaller gibi farklı gruplar oluşturmak için tasarlanmış bir eklentidir. Daha fazla bilgi için, [burayı tıklayın](#) [224]

#### 5.5.3 DuckDuckGo



[225]

**DuckDuckGo** **Google** ve **Bing** gibi arama motorlarına daha gizli ve güvenli bir alternatif sunmak için tasarlanmıştır. **DuckDuckGo** kullanıcı bilgilerini kayıt altına almaz ve paylaşmaz ve bütün kullanıcıların aynı bilgilere erişimi olmasını sağlar. **DuckDuckGo** [226] web sitesine doğrudan giderek veya **DuckDuckGo** ikonuna tıklayarak kurabilir ve arama sekmesindeki otomatik arama motorunuz haline getirebilirsiniz.

#### 5.5.4 vtzilla



[227]

**vtzilla** indirilenleri ve web sitelerini kötücül yazılım ve virüs olup olmadığını anlama amaçlı taramak için tasarlanmıştır. **Vtzilla** eklentisini başarılı bir şekilde kurduktan sonra, **Firefox** arama araç çubuğunun altında **vtzilla** araç çubuğu belirir (ki bu istenirse kaldırılabilir). **Vtzilla** arama kutusuna bir web sitesi adresi yapıştırabilir ve arama isteğinizin **Virus Total** web sitesine yönlendirilmesini sağlayabilirsiniz. Bu web sitesi belirlenen bağlantı veya web sitesine 40'tan fazla kötücül yazılım ve virüs tarayıcısı yönlendirir. Buna ek olarak, **vtzilla**, indirdiğiniz dosyaları da tarayarak var olan anti-virüs programlarına (örneğin **avast!** [228] gibi) ek bir güvenlik getirir ve bu sayede bilgisayarınızın korunmasını artırır. Daha fazla bilgi için, [burayı tıklayın](#) [229].

### 5.5.5 ShareMeNot



[230]

**ShareMeNot** İnternet üzerindeki sitelere eklenmiş olan üçüncü tarafların düğmelerinin (örneğin Facebook 'Beğen' düğmesini veya Twitter 'tweet' düğmesi), siz onlara basana kadar sizi takip etmesini engellemek üzere tasarlanmıştır. Daha fazla bilgi için, [burayı tıklayın](#) [231].

### 5.5.6 Click&Clean



[232]

**Click&Clean Firefox'u** kapattığınız anda kişisel verilerinizin silinmesi için tasarlanmıştır. Buna, indirilenler tarihiniz, tarama tarihiniz ve **Flash Local Shared Objects (LSO)** gibi çerezler de dahildir. Ayrıca, geçici dosyaları siler ve lokal önbelleğinizi de temizler.

**Not:** Buna alternatif olarak, **Windows** işletim sistemi için **CCleaner** [233], **Wise Disk Cleaner** veya **Linux** için **Janitor** veya **BleachBit** gibi harici uygulamalar da kullanabilirsiniz.

## Taşınabilir Firefox

### Kurulu ve Taşınabilir Firefox arasındaki farklar

Taşınabilir araçlar, lokal bilgisayarlara kurulmadıkları için fark edilmeden kullanılabilirler. Fakat aklınızda tutun ki, harici araç ve USB bellek çubukları ancak bilgisayarınız kadar güvenlidir ve reklam destekli yazılım, kötücül yazılım ve virüslere maruz kalabilir.

**Mozilla Firefox Taşınabilir Sürüm** ve lokal bir bilgisayara kurulabilir olan sürüm arasında fark yoktur.

### 2.0 Taşınabilir Firefox Nasıl İndirilir ve Pakitinden Çıkartılır?

**Taşınabilir Firefox'u** indirmek ve çıkarmak için aşağıdaki adımları takip ediniz :

**1. Adım.** Uygun indirme sitesine ulaşmak için [http://portableapps.com/apps/internet/firefox\\_portable](http://portableapps.com/apps/internet/firefox_portable) [234] adresine **tıklayın**.

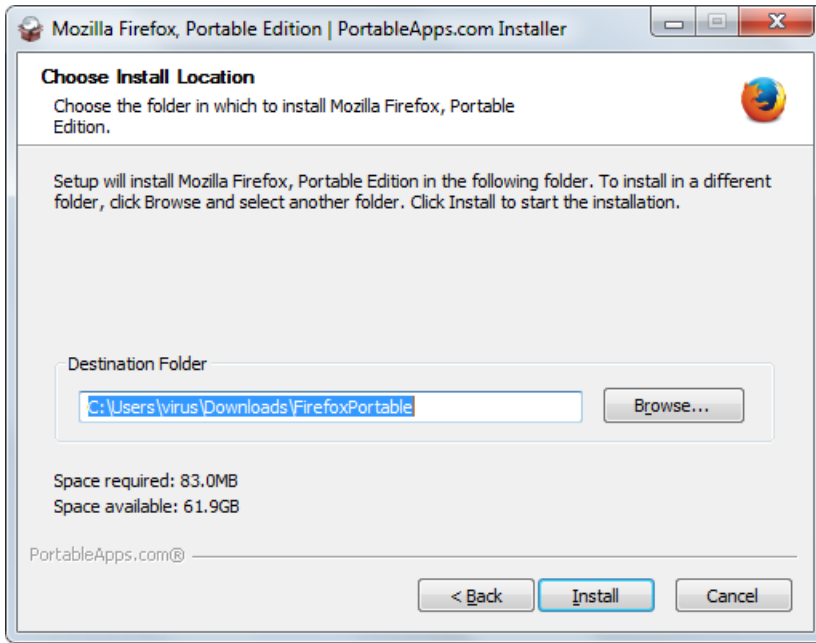


**2. Adım.** **Taşınabilir Firefox** kurulum dosyasını indirmek için **tıklayın**.

**3. Adım.** **FirefoxPortable\_38.0\_English.paf** kurulum dosyasını bilgisayarınıza kaydetmek için **Kaydet** 'i **tıklayın** ve kaydettiğiniz yere **gidin**.

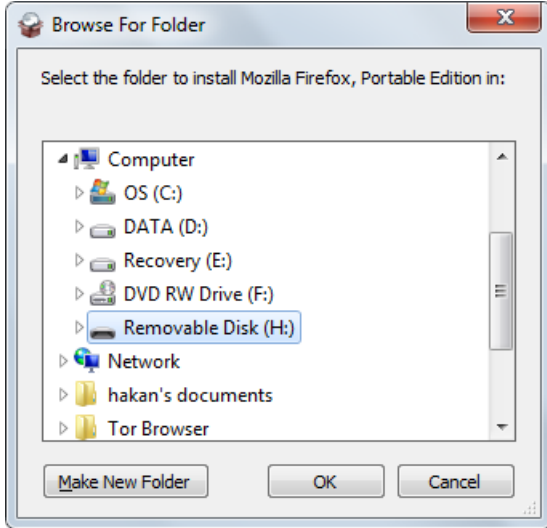
**4. Adım.** **FirefoxPortable\_38.0\_English.paf** 'e **çift tıklayın**. **Dosyayı Aç – Güvenlik Uyarısı** kutusu açılırsa **Mozilla Firefox – Portableapps.com Kurucusu** penceresini etkinleştirmek için **Çalıştır** 'i **tıklayın**.

**5. Adım.** Aşağıda görünen ekranı etkinleştirmek için **Next >** 'i **tıklayın**:



Şekil 2: Kurulum Konumunu Seç penceresi

6. Adım. Klasörleri Tara penceresini aşağıdaki gibi etkinleştirmek için **Gözet...** butonuna tıklayın:

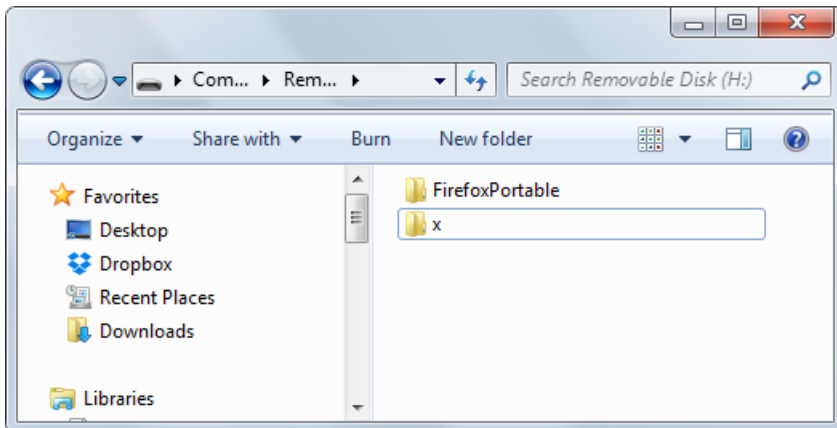


Şekil 3: Klasör Tara penceresi

7. Adım. Harici araç veya USB bellek çubuğuna **gidin** ve yukarıdaki Şekil 3'te görüldüğü gibi, **Mozilla Firefox Taşınabilir Sürüm** klasörünü onaylamak için **OK** butonuna tıklayın. Kurulum Konumunu Seç penceresine geri dönün.

8. Adım. Çıkarma işlemine başlamak için **Install** butonuna tıklayın ve kurulum işlemi tamamlamak için **Finish** butonuna tıklayın. Daha sonra, **Mozilla Firefox Taşınabilir Sürüm** klasörünün kaydedildiği harici araç veya USB bellek çubuğuna **gidin**.

9. Adım. Çıkarılabilir araç veya USB bellek çubuğunuzu **açın**. Aşağıdaki gibi bir ekran göreceksiniz:



Şekil 4: Yeni kurulmuş Mozilla Firefox Taşınabilir Sürüm ve mavi ile işaretlenmiş Taşınabilir Firefox klasörü

**10. Adım. Taşınabilir Firefox** klasörünü **açın** ve **Taşınabilir Firefox'u** kullanmaya başlamak için  FirefoxPortable.exe'ye **çift tıklayın**.

Yapılandırma ve kullanma için lütfen **Firefox** <sup>[86]</sup> bölümüne başvurun.

#### Offline Installation Instructions :

##### Firefox'u Kurma

- Kısa [Uygulamalı-Rehber'in](#) <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Firefox** ikonlarını **tıklayın** ve kurucuları 'Açın' ya da 'Çalıştırın'. Gerekirse önce kurucuyu indirin ve sonra yerini bulup üstüne çift tıklayın
- Devam etmeden önce bir sonraki kısımdaki 'Kurulum Yönergeleri'ni okuyun
- Kurucuyu bilgisayarınıza kaydettiyseniz kurulumdan sonra silebilirsiniz

Firefox:



[235]

## Sıkça Sorulan Sorular ve Gözden Geçirme

### 6.0 Sıkça Sorulan Sorular ve Gözden Geçirme

**Soru:** Kendimi kötücül yazılım içeren web sitelerinden korumak için neden bu kadar çok eklentiye ihtiyacım var? Örneğin, **NoScript** tehlikeli kodlara karşı koruma sağlıyorsa, benzer işlevlere sahip olan diğer eklentilere neden ihtiyacım var?

**Cevap:** Genel güvenlik konuları ile başa çıkmak için birden fazla araç kullanmak faydalıdır. (Anti-virüs programları buna istisna oluşturur çünkü bu programlar birbirleri ile uyumsuzdurlar.) Bu Firefox eklentileri, tarayıcınızı çok çeşitli tehlikelerden farklı teknikler kullanarak korurlar. Örneğin, **NoScript** bilinmeyen sitelerden gelen kodları engeller, fakat kullanıcılar sık ziyaret ettikleri web sitelerini 'beyaz liste'ye alma eğilimindedirler ve bu sitelerden potansiyel kötücül kodlar gelmesi muhtemeldir. Buna ek olarak, **NoScript** kullanıcıları, geçici olarak, sayfanın düzgün bir şekilde çalışması için bilinmeyen sitelerin kod yüklemesine de izin verebilirler.

### 6.1 Gözden Geçirme Soruları

- Geçici İnternet geçmişi, çerezler ve tarayıcı önbelleği nasıl silinir?
- **NoScript** sisteminizi ne tür tehlikelerden korur?

## Tor Tarayıcı - Digital Anonimlik ve Atlatma

#### Short Description:

**Tor Tarayıcı** internetteki etkinliklerinizin anonimliğini artırmak için tasarlanmıştır. Kimliğinizi gizler ve çevrimiçi etkinliklerinizi internet gözetlemeciliğinin birçok şeklinden korur. **Tor** internet filtrelerini atlatmanızı da sağlar.

#### Online Installation Instructions:

##### Tor Tarayıcı'yı İndirme

- Kısa [Uygulamalı Rehberler'in](#) <sup>[1]</sup> giriş bölümünü okuyun
- Aşağıdaki **Tor** ikonunu **tıklayarak** <https://www.torproject.org/easy-download.html.en> sayfasını açın
- Sayfayı **aşağı kaydırın** ve **Microsoft Windows için Tor Tarayıcı** linkini tıklayın
- Çalıştırılabilir dosyayı **kaydedin** ve yerini **bulup** üstüne **çift tıklayın**
- **Tor Tarayıcı'yı** paketinden çıkarttıktan sonra bilgisayarınıza kaydettiğiniz bu çalıştırılabilir dosyayı silebilirsiniz

Tor:



[236]

**Not:** Tor Projesi websitesine ulaşımın engellendiği bir bölgedeseyeniz, **Tor Tarayıcı Paketi'nin** kopyasını e-posta ile talep edebilirsiniz. Bunu yapmak için [gettor@torproject.org](mailto:gettor@torproject.org) adresine talep ettiğiniz tor versiyonunu da belirttiğiniz bir e-posta atın. Mesela bilgisayarınız Windows'la çalışıyorsa **windows**, Apple'la çalışıyorsa **osx** ya da Linux'la çalışıyorsa **linux**

versiyonu diyebilirsiniz. **Dropbox** aracılığıyla kurucuyu indirebileceğiniz bir linki içeren bir e-posta cevabı alacaksınız. Bu özelliğe dair daha fazla detayı [Tor Projesi websitesinde](https://www.torproject.org) <sup>[237]</sup> bulabilirsiniz.

## Ana Sayfa

<https://www.torproject.org> <sup>[238]</sup>

## Bilgisayar Gereksinimleri

- İnternet bağlantısı
- Bütün Windows sürümleri (XP ve sonrasındakiler)

## Bu rehberde kullanılan sürümler

- Tor Tarayıcı: 3.5.3

## Bu bölümün son güncellenme tarihi

- Mart 2014

## Lisans:

- Ücretsiz ve Açık-Kaynak Yazılım

## Gerekli Okuma

- Nasıl Yapmalı Kitapçığının **8. İnternette nasıl anonim kalınır ve internet sansürü nasıl aşılr** <sup>[75]</sup> bölümü

## Buradan sağlayacağınız faydalar:

- Ziyaret ettiğiniz websitelerinden digital kimliğinizi gizleme yetisi
- **İnternet Servis Sağlayıcıları (Internet Service Providers, ISPs)** ve diğer gözetleme mekanizmalarından çevrimiçi taramalarınızı gizleme yetisi
- İnternet sansür ve filtreleme kurallarını atlatma yetisi

## GNU Linux, Mac ve Microsoft Windows'a Uyumlu Diğer Programlar

Tor Tarayıcı GNU Linux, Mac OS, Microsoft Windows ve Android işletim sistemleri için ulaşımdaydır. Tor çevrimiçi aktivitelerinizin anonimliğini korumak için en çok tavsiye edilen ve dikkatli bir şekilde test edilen araçtır. Yine de tavsiye edilen diğer çözümlerden bazılarını da burada listelemek isteriz.

- **Riseup VPN** <sup>[239]</sup> **Linux, MAC, Android ve Microsoft Windows** için ücretsiz bir Sanal Gizli Ağ (Virtual Private Network, VPN) proxy sunucusudur.
- **Psiphon3** <sup>[240]</sup> **Microsoft Windows ve Android OS** ücretsiz ticari bir **Sanal Gizli Ağ (VPN)** çözümüdür.
- **Dynaweb FreeGate** <sup>[241]</sup> **Microsoft Windows** için ücretsiz bir proxy aracıdır.
- **Your Freedom** <sup>[242]</sup> da ücretsiz (ama daha yavaş) bir servis sunan ticari bir proxy aracıdır. **Linux, Mac OS ve Microsoft Windows** için ulaşımaya açıktır.

## 1.1 Başlamadan önce bu araç hakkında bilmeniz gerekenler

**Tor Tarayıcı** internet aktiviteleriniz ve alışkanlıklarınızın gizliliği ve güvenliğini artırmak için tasarlanmış bir yazılım aracıdır. Kimliğinizi ve çevrimiçi taramalarınızı internet gözetlemecilerinin pek çok formundan saklar. **Tor** elektronik kısıtlamaları atlatmanın da güvenli bir yolu olarak faydanıza sunulur ki bloglara ya da haberlere ulaşımınız ya da bunları yayınlamanız mümkün olsun.

**Tor** dünyanın her yerine yayılmış gönüllülerin çalıştırdığı sunucu ağı içinde iletişimleri rotalandırarak *anonimliğinizi* korur. **Tor'u** kullanmak ziyaret ettiğiniz siteleri potansiyel gözetlemecilerden sakladığı gibi, sizin kimliğinizi ve bulunduğunuz yeri o ziyaret ettiğiniz sitelerden gizler. Yazılım, **Tor** ağı içindeki sunucuların hiçbirinin **hem** yerinizi **hem de** ziyaret ettiğiniz siteleri **bilmemesini** sağlayacak şekilde tasarlanmıştır.

**Tor** kendisine gelen ve kendi ağı içinde ilerleyen iletişimin de şifrelenmesi için adımlar atmaktadır, **fakat** bu önlem şifrelenmemiş kanallardan (https ulaşımı vermeyen) içerik alıp gönderen bir web siteye kadar işleyemez. Yine de bu tür sitelere **Tor** kullanarak ulaşmanın faydası **Tor'un** iletişiminizi **Tor sunucularından** o güvenliksiz sitelere atılan son adıma kadar iletişiminizi koruyor olmasıdır. Böylece iletişiminizin içeriğinin gözlenme ihtimali sadece bu son adıma kısıtlanır.

Tor Tarayıcı Paketi Tor yazılımı ve kullanımı esnasında ekstra güvenlik sağlaması için tasarlanmış Firefox web tarayıcısının modifiye edilmiş bir sürümünü içerir. Bu paket aynı zamanda **NoScript** <sup>[243]</sup> and **HTTPS-Everywhere** <sup>[244]</sup> eklentilerini de barındırır.

**Not:** Anonimliğin korunması bir miktar hız kaybı pahasına sağlanır. Tor taramalarınızın anonimliğini internet trafiğinizi dünyanın farklı yerlerindeki gönüllülerin bilgisayarları ve sunucuları arasında dolandırarak koruduğu için kesinlikle bilgisayarınızdaki diğer web tarayıcılarından daha yavaş işleyecektir.

## Tanımlar:

- **Köprü Durağı:** Köprü Durağı kaynağı gizli tutulan bir **Tor** sunucusudur. Bir köprü kullanmayı seçerseniz, sunucu size **Tor** ağına ulaşma imkanı verir, **Tor** bulunduğunuz ülkede engellenmiş olsa bile.
- **Port:** Bu bölümde, port yazılımın ağıdaki diğer bilgisayarlarda çalışan servislerle iletişiminin kurulduğu bir ulaşım noktasıdır. Bir URL, mesela **www.google.com**, bir servisin sokak adresini bilmenizi sağlıyorsa, port size hedefinize ulaştığınızda hangi kapıyı kullanmanız gerektiğini söyler. İnternet taramaları esnasında güvenli olmayan siteler için (**http://mail.google.com**) genelde port 80 kullanılırken, port 443 güvenli siteler için kullanılır (**https://mail.google.com**).
- **Proxy:** Proxy bilgisayarınızda, yerel ağızda ya da internette başka bir yerde çalışan bir aracı yazılımdır, iletişiminizin hedefine giderken yönlendirilmesine yardımcı olur.
- **Rota:** Rota bilgisayarınız ile hedef sunucu arasındaki internet iletişim yoludur.

#### Offline Installation Instructions :

#### Tor Tarayıcıyı Kurma

- *Kısa Uygulamalı Rehberler'in* <sup>[1]</sup> Giriş bölümünü okuyun
- Aşağıdaki **Tor** ikonunu **tıklayın** ve kurucuyu 'Açın' ya da 'Çalıştırın'. Gerekirse, önce kurulumcuyu kaydedin, sonra kaydettiğiniz yeri bulup üstüne çift tıklayın
- Kurucuyu bilgisayarınıza kaydettiyseniz, kurulumdan sonra silebilirsiniz

Tor:



[245]

## Tor Tarayıcı nasıl paketinden çıkartılır?

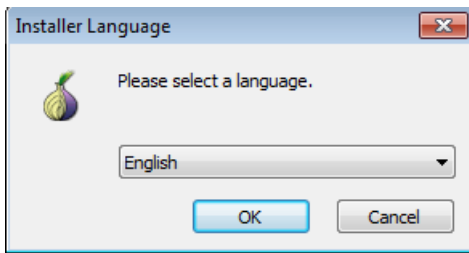
### 2.0 Tor Tarayıcı Nasıl Paketinden Çıkartılır

**Tor Tarayıcı** internette anonim bir şekilde gezinmeniz için ihtiyacınız olan herşeyi sunan **Firefox'un** modifiye edilmiş bir versiyonudur. Bu paket kurulum gerektirmez, sadece paketinden çıkartılması ve çalıştırılması gerekir.

**Tor Tarayıcı'yı** paketinden çıkarmak için aşağıdaki adımları takip edin:

**1. Adım.**  **torbrowser-install-4.5.1\_tr** 'ye **çift tıklayın**. Dosyayı Aç – Güvenlik Uyarısı kutusu açılırsa **Çalıştır** 'ı **tıklayarak** programı etkinleştirin.

Bundan sonra dil seçimi ekranı belirecek.



Şekil 1: Dil seçimi ekranı

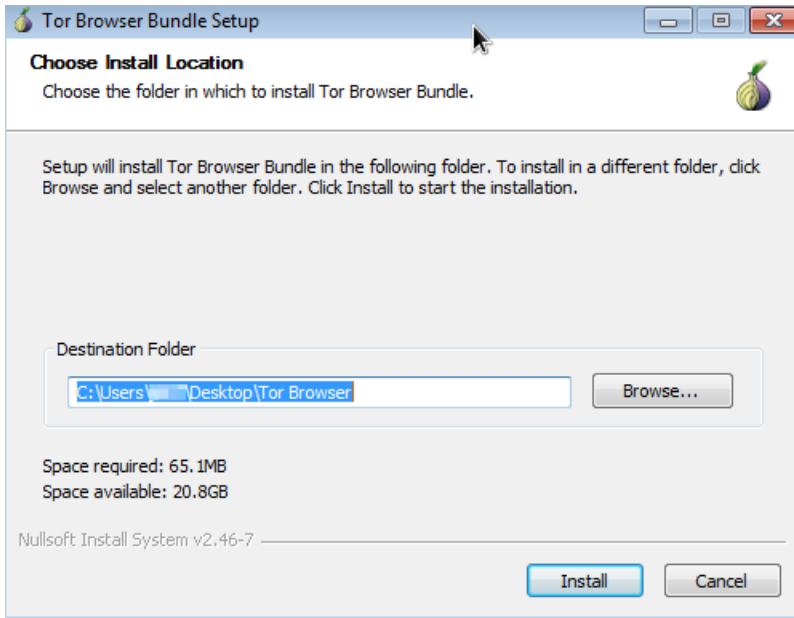
Aşağı açılır menüden dilinizi **seçin** (henüz Türkçe sürümü olmadığı için İngilizce sürümü seçebilirsiniz) ve **Tamam'ı** **tıklayarak** aşağıdaki ekranı etkinleştirin.

**2. Adım.** **Tor Tarayıcı'yı** çıkartmak istediğiniz yeri **seçin**.

Not: **Tor Tarayıcı** C: \Programlar klasörüne kurulmaz (tavsiye ettiğimiz araçların çoğunun kurulum prosedürlerinin aksine) bunun yerine *Masaüstünde* bir klasör yaratır.

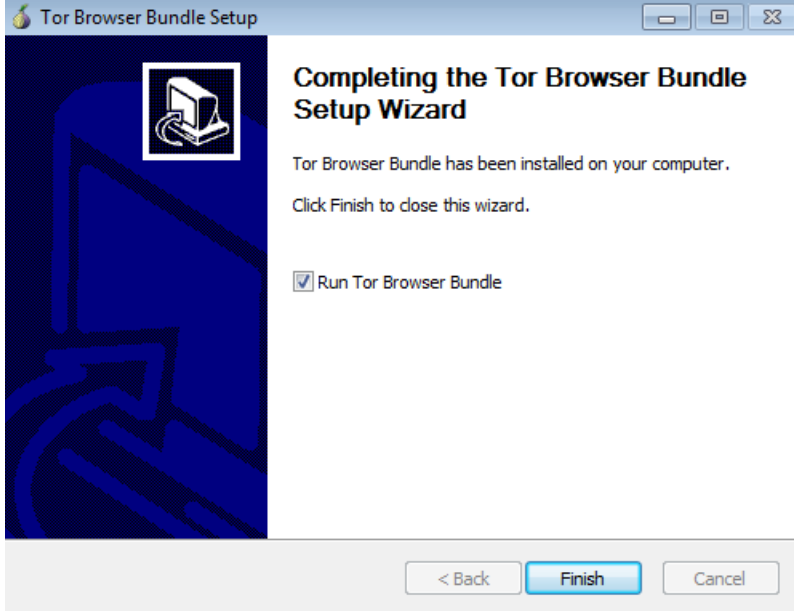
**Önemli:** **Tor Tarayıcı'yı** bilgisayarınızda başka bir dosya ya da USB bellek çubuğuna da çıkartabilir ve oradan kullanabilirsiniz. Bu bilgisayarınızda **Tor** kullandığınız gerçeğini saklamanıza yardımcı olabilir.

Ya **Install** 'ı **tıklayarak** verili seçenek olan *Masaüstü'nü* kabul edin ve aşağıdaki pencereyi etkinleştirin, ya da, **Browse...** 'ı **tıklayarak** *Klasöre Göz At* penceresini etkinleştirin ve **Tor Tarayıcı'yı** çıkartmak istediğinizi yere doğru ilerleyin.



Şekil 2: Tor Tarayıcı için verili olan çıkarma yerinin bir örneği

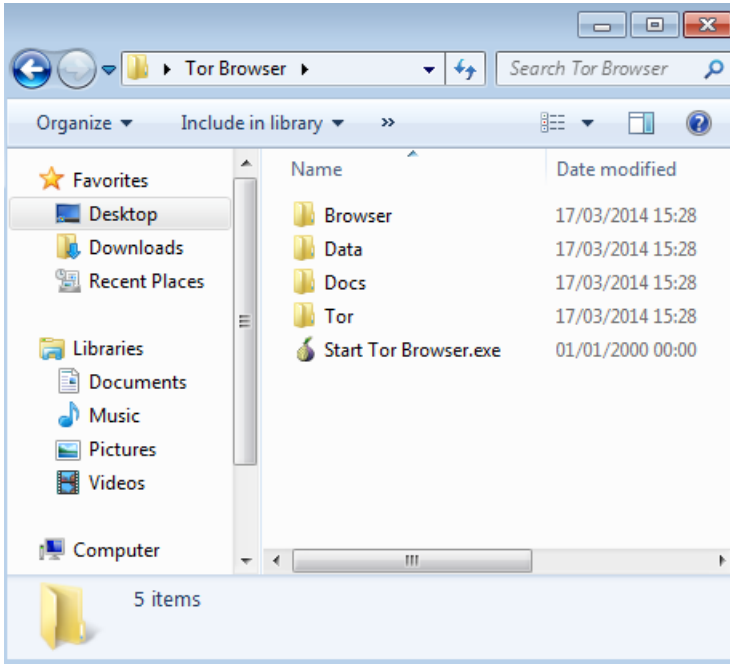
3. Adım. **Install** butonunu tıklayarak Tor Tarayıcı'yı çıkartmaya başkayın. Çıkartma işlemi bittiğinde Tor Tarayıcı'nın kurulduğunu teyit eden ve onu hemen başlatma seçeneğini sunan bir ekran açılacak.



3. Şekil: Çıkartma işlemi başarıyla tamamlandı

Dikkat edin ki yukarıdaki şekilde Tor Tarayıcı'yı Çalıştır seçeneği işaretlenmiş. Bitir düğmesini tıkladığınızda Tor Tarayıcı otomatik olarak açılacak.

Bu örnekte, Tor Tarayıcı çıkartma işlemi tamamlandıktan sonra, Masaüstünde Tor Tarayıcı isimli bir klasörde bulunacak. Ne zaman Tor Tarayıcı'yı kullanmak isterseniz Start Tor Browser.exe 'ye çift tıklamanız yeterli.



4. Şekil: Masaüstünde bir klasöre çıkartılmış Tor Tarayıcı

Şimdi **Tor Tarayıcı'yı** başarıyla çıkarttınız.

## Tor Tarayıcı'yı Kullanarak İnternete Nasıl Ulaşabilirsiniz?

- **3.0 Tor Ağı'na Nasıl Bağlanabilirsiniz?**
- **3.1.1 - Direkt Erişim**
- **3.1.2 - Kısıtlı Erişim**
- **3.2 Tor Ağına Erişimi Yeniden Yapılandırma**
- **3.3 Köprü Adreslerini Alma**

### 3.0 Tor Ağı'na Nasıl Bağlanabilirsiniz?

**Tor Tarayıcı'yı** ilk defa çalıştırdığınızda internete nasıl bağlanmak istediğiniz sorulacak:

- **Direkt Erişim:** Bu seçenek bulunduğunuz yerde internete erişiminiz kısıtlanmamış ve **Tor** kullanımı bloke edilmemiş, yasaklanmamış, ya da kontrol altında tutulmamış ise seçilmelidir.
- **Kısıtlı Erişim:** Bu seçenek bulunduğunuz yerde internete erişiminiz kısıtlanmış ise ya da **Tor** kullanımı bloke edilmiş, yasaklanmış ya da kontrol altına alınmış ise seçilmelidir.

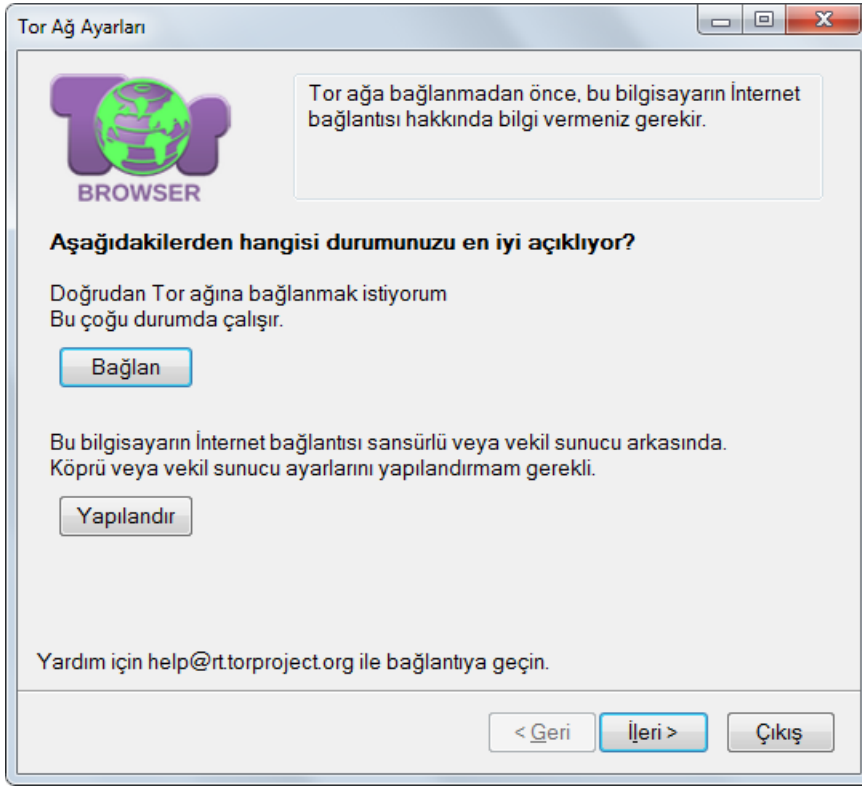
Bu ayarlar **Tor Tarayıcı'nın** içinden, yazılımı yeniden kurmadan, herhangi bir zamanda değiştirilebilir. Bu, bulunduğunuz konumdaki şartlar değiştiği zaman ya da farklı bir ülkeyi ziyaret ediyorsanız yapmanız gereken bir şey olabilir.

Daha sonra, **Tor Tarayıcı'yı** başlattığınız zaman, ek bir yapılandırma gerektirmeden **Tor** ağına bağlanmanızı sağlayacaktır.

### 3.1.1 Tor Ağına Nasıl Bağlanabilirsiniz? - Direkt Erişim

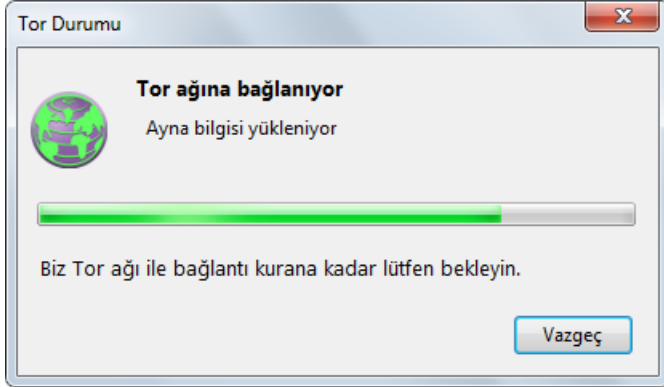
**Tor Tarayıcı'yı**, **Tor** ağına direkt olarak erişecek şekilde yapılandırmak için aşağıdaki adımları takip etmelisiniz:

**1.Adım.** *Tor Tarayıcı* klasörüne **gidin** ve **Start Tor Browser.exe** 'yi **çift tıklayın**. Aşağıdaki ekranı göreceksiniz:



Şekil 1: Tor Ağ Ayarları paneli

**2. Adım.** **Bağlan** düğmesini **tıklayın** ve **Tor Statüsü** penceresini açın. Bu pencereden, yazılımın **Tor Ağına** bağlanma gelişimini görebilirsiniz.



Şekil 2: Tor statüsü penceresi ve bağlanma gelişimi

Birkaç saniye sonra, **Tor Tarayıcı**, aşağıdaki ekranı gösteren yeni bir tarayıcı penceresini etkin kılacaktır:



Şekil 3: Tor ağına başarılı bir şekilde bağlanmış Tor Tarayıcı

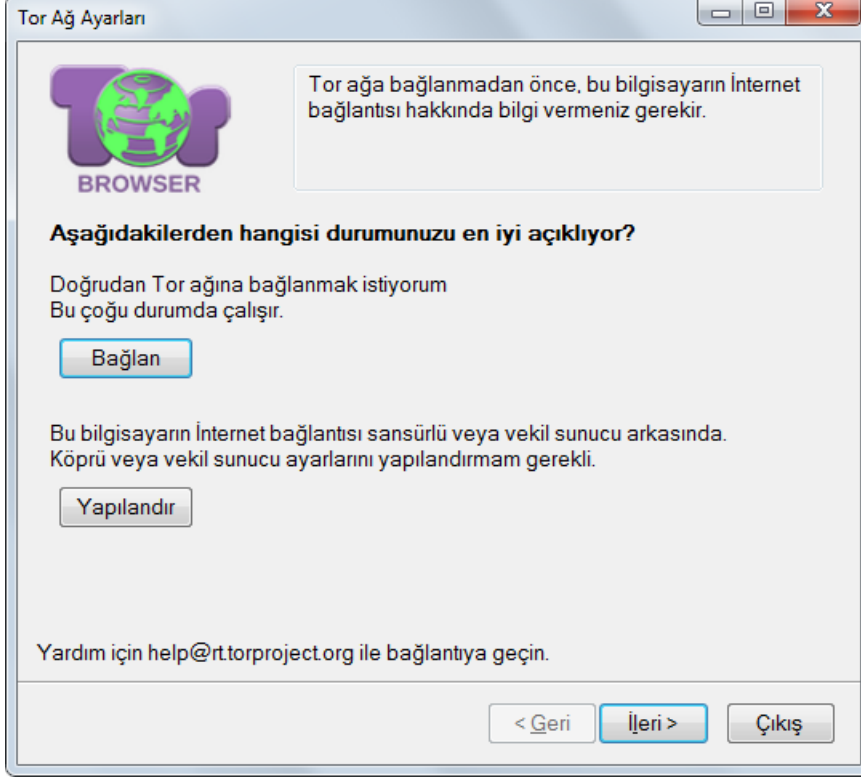
Şimdi, web'i **Tor ağı** güvenliği ile tarayabilirsiniz.

**Not: Tor Tarayıcı'yı** her başlattığınızda, *Tor Tarayıcı* başlamadan önce (Şekil 3) otomatik olarak Tor Statüsü penceresi (Şekil 2) açılacaktır.

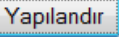
### 3.1.2 Tor Ağına Nasıl Bağlanabilirsiniz? - Kısıtlı Erişim

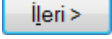
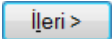
Tor Ağına erişimin, yukarıda tarif edildiği gibi, mümkün olmadığı ya da riskli olduğu bir bölgede yaşıyorsanız, Tor'u bu engelleri aşacak şekilde yapılandırmayı deneyebilirsiniz.

**1. Adım:** *Tor Tarayıcı* klasörüne idin,  *Start Tor Browser.exe* 'yi **çift tıklayın** ve aşağıdaki ekranı etkinleştirin:

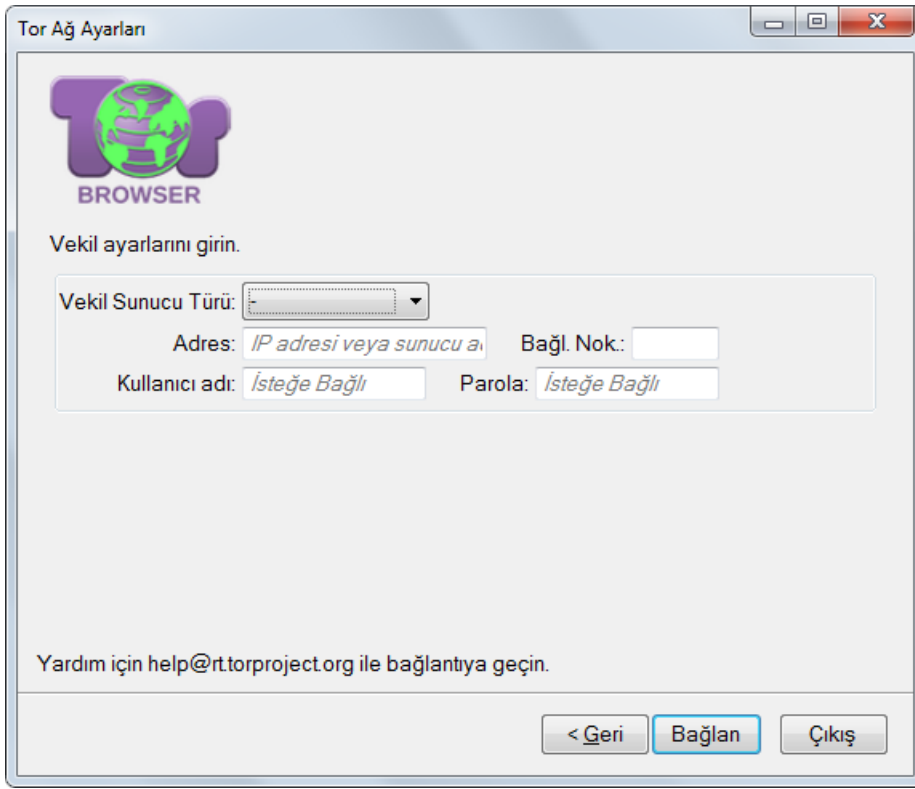


Şekil 4: Tor Ağı Ayarlar paneli

**2. Adım:**  düğmesini **tıklayın** ve yeni bir pencere açın. **Tor Ağına** erişmenize yardımcı olacak üç kısa yapılandırma sorusu sorulacak.

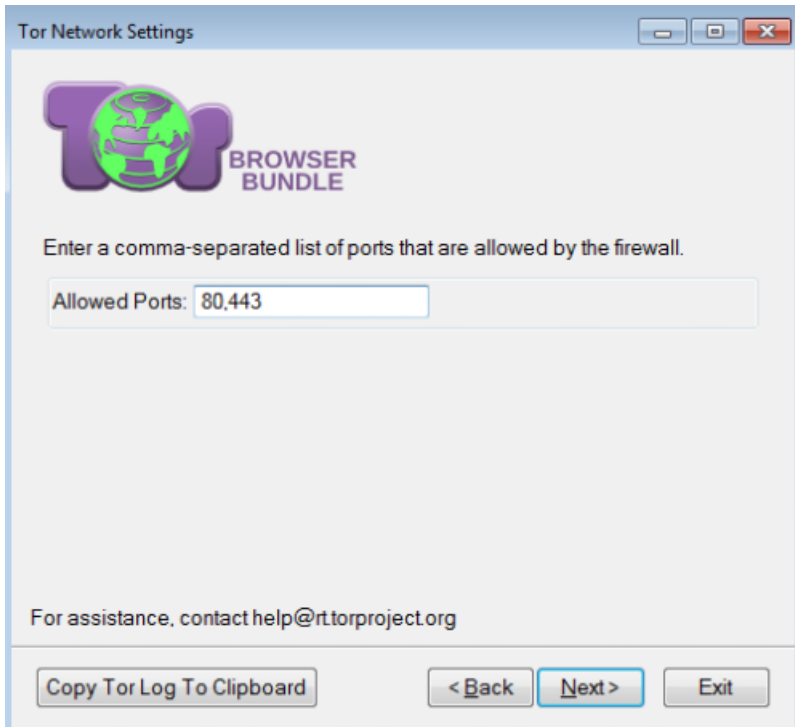
**1. Soru: Proxy Erişimi;** İnternete proxy üzerinden erişmeniz gerekiyorsa **evet'i** işaretleyin ve  'e basın. Proxy kullanmıyorsanız, **hayır'ı** işaretleyin ve  'e basın.

Yukarıda **evet'i** işaretlediyseniz, bir sonraki ekranda proxy ayarlarınızı girin. Proxy ayarlarınızı bilmiyorsanız, her zaman kullandığınız tarayıcı ayarlarına bakın. **Firefox'ta** ayarları, *Bağlantı Ayarları* bölümünde *Seçenekler>Gelişmiş>Ağ* sekmesi'nde bulabilirsiniz. Diğer tarayıcılarda, *İnternet Seçenekleri* bölümüne bakabilirsiniz. Daha fazla yardım için tarayıcınızdaki *Yardım* özelliğini kullanabilirsiniz.



Şekil 5: Proxy ayarları ekranı

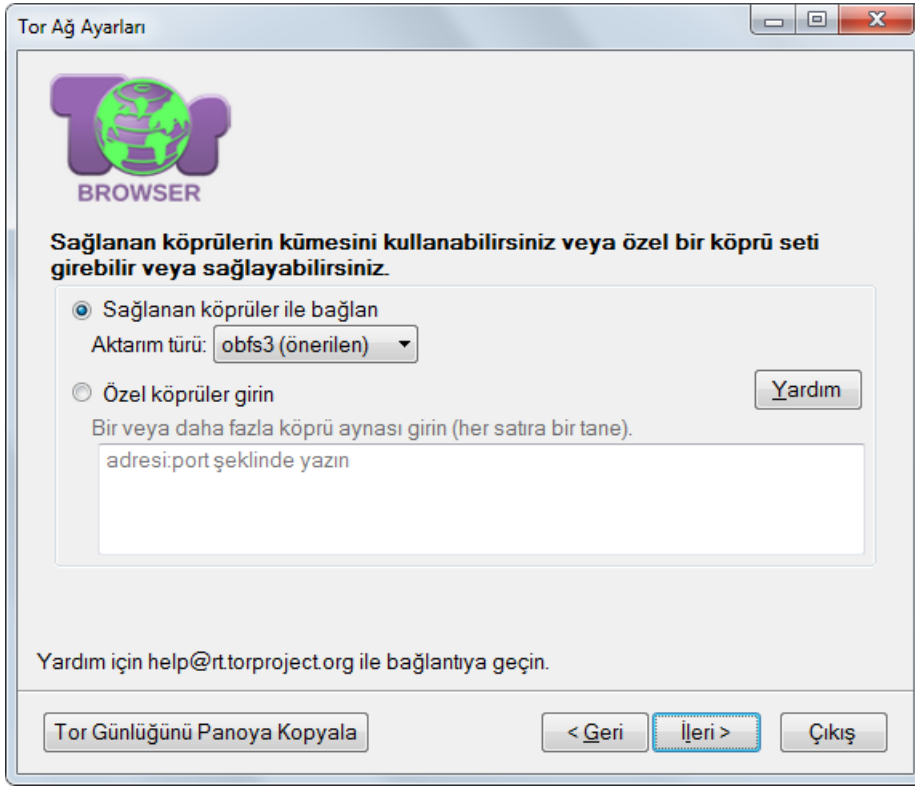
**Soru 2: Kısıtlı Portlar**, İnternet'e, web tarama için, *port 80 ya da 443* gibi, sadece belli portlara erişime olanak veren bir güvenlik duvarı üzerinden erişiyorsanız, **evet**'i seçin ve portları yapılandırmak için **İleri >** ye basın. Durum bu değilse, **hayır**'ı seçin ve **İleri >** 'e basın.



Şekil 6: Port kısıtlama yapılandırma ekranı

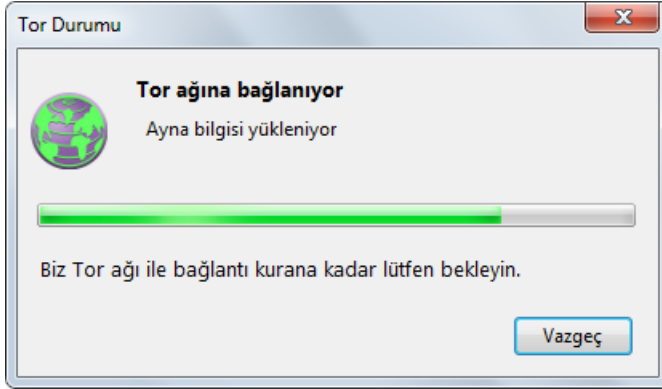
**Soru 3: Sansürlü İnternet bağlantısı**, **Tor** trafiğini aktif olarak engelleyen veya denetleyen bir ülkede yaşıyorsanız, **Tor** kullandığınızı gizleyen bir **Köprü** kullanarak **Tor Tarayıcısı**'nı yapılandırabilirsiniz.

2. sorudan sonra **İleri >** 'i tıklayınca, **Köprü adreslerini** girmenize izin veren bir ekranla karşılaşacaksınız. Köprü adresleri almak ile ilgili daha fazla bilgi almak için **Köprü Adresleri Alma** bölümüne bakabilirsiniz.



Şekil 7: Tor Bridge etkinleştirme ekranı

Köprü adreslerini ekledikten sonra yapılandırmanızı bitirmek için **Bağlan** butonunu tıklayın ve **Tor Ağına** bağlanın.



Şekil 8: Tor Statüsü pencereleri ve bağlantı gelişimi

Birkaç saniye sonra, **Tor Tarayıcı**, aşağıdaki ekranı gösteren yeni bir tarayıcı penceresi etkinleştirecek:



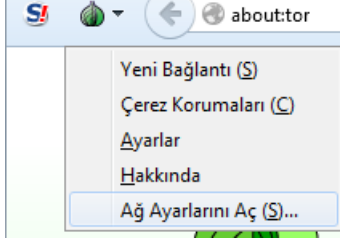
Şekil 9: Tor ağına başarılı bir şekilde bağlanmış Tor Tarayıcı

Şimdi **Tor ağı** koruması ile web'i tarayabilirsiniz.

**Not: Tor Tarayıcı'yı** her başlattığınızda, *Tor Tarayıcı'dan önce (Şekil 9) otomatik olarak Tor Statü penceresi* açılacaktır (Şekil 8).

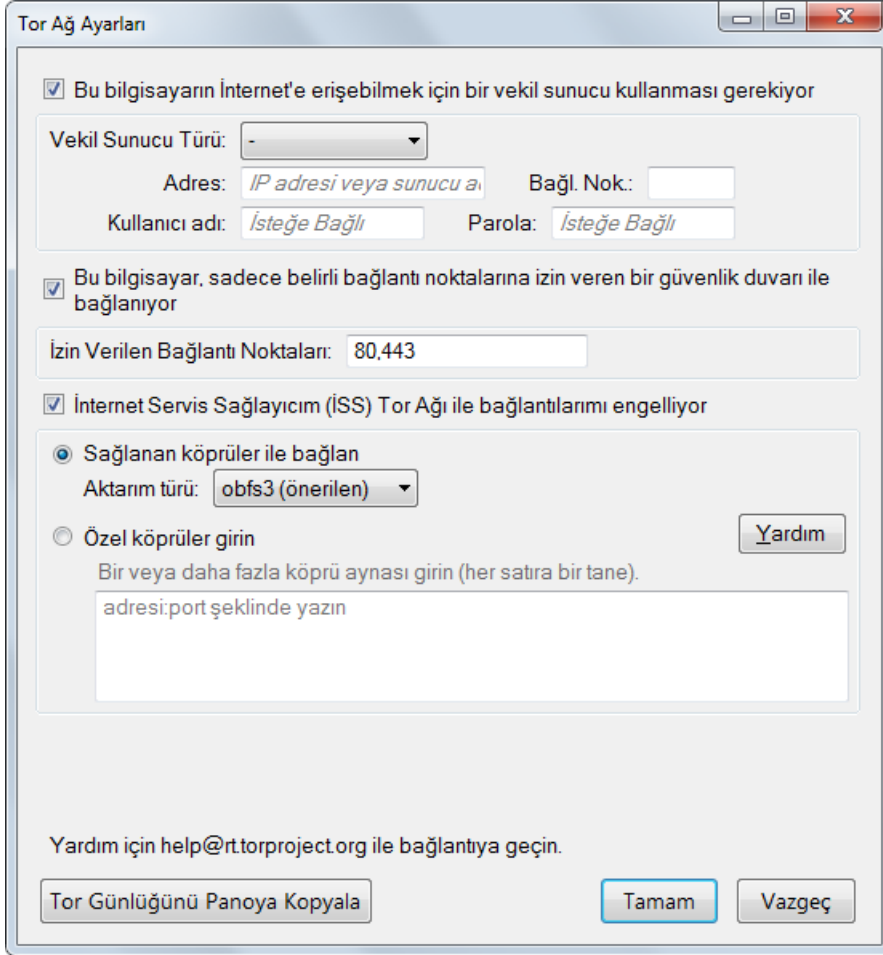
## 3.2 Tor Ağına erişimi yeniden yapılandırma

Herhangi bir noktada, **Tor Ağı'na** farklı bir şekilde bağlanmanız gerektiğinde mesela Tor'a erişimi engelleyen bir ülkeye gittiğiniz zaman, Tor Ağına farklı bir şekilde erişmeniz gerektiğinde, tarayıcı içerisinde ayarlarınız güncelleyebilirsiniz.  ikonunu tıklayın ve **Ağ Ayarlarını Aç (S)...** seçin.



Şekil 10: Tor Tarayıcı seçenekleri

**Tor Tarayıcı'nın** İnternet'e erişme şeklini değiştirmenize olanak veren yeni bir pencere açılacak (Şekil 11). İsteddiğiniz seçenekleri işaretleyin ve ayarları değiştirin. İsteddiğiniz değişiklikleri yaptıktan sonra **Tamam** 'e basın ve **Tor Tarayıcı'yı** yeniden başlatın.



The 'Tor Ağ Ayarları' window contains the following settings:

- ☒ Bu bilgisayarın İnternet'e erişebilmek için bir vekil sunucu kullanması gerekiyor
- Vekil Sunucu Türü: -
- Adres: IP adresi veya sunucu adı
- Bağl. Nok.:
- Kullanıcı adı: İsteğe Bağlı
- Parola: İsteğe Bağlı
- ☒ Bu bilgisayar, sadece belirli bağlantı noktalarına izin veren bir güvenlik duvarı ile bağlanıyor
- İzin Verilen Bağlantı Noktaları: 80.443
- ☒ İnternet Servis Sağlayıcım (İSS) Tor Ağı ile bağlantılarımı engelliyor
- ☒ Sağlanan köprüler ile bağlan
- Aktarım türü: obfs3 (önerilen)
- ☐ Özel köprüler girin
- Yardım
- Bir veya daha fazla köprü aynası girin (her satıra bir tane).
- adres:port şeklinde yazın
- Yardım için [help@rt.torproject.org](mailto:help@rt.torproject.org) ile bağlantıya geçin.
- Tor Günlüğünü Panoya Kopyala
- Tamam
- Vazgeç

Şekil 11: Tor Tarayıcı seçenekleri

## 3.3 Köprü Adreslerini Alma

**Tor Tarayıcı'yı Köprüleri** kullanmak üzere yapılandırmak için köprü adresleri almanız gerekir. Bunu yapmanın iki yolu vardır:

### E-posta:

Köprüleri E-posta yoluyla almak için, Gmail ya da Yahoo hesabına sahip olmanız gerekir. [bridges@bridges.torproject.org](mailto:bridges@bridges.torproject.org) adresine *get bridges* konulu bir e-posta gönderin. Birkaç dakika sonra, 3 köprünün ve diğer detayların yer aldığı bir e-posta alacaksınız.

to me 

Here are your bridge relays:

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable.

transport NAME : request transport NAME. Example: "transport obfs2"

Another way to find public bridge addresses is to visit <https://bridges.torproject.org/>. The answers you get from that page will change every few days, so check back periodically if you need more bridge addresses.

**Web Sites:**

Websitesini açtıktan sonra üç adım takip etmelisiniz:

- 'ı tıklayın
- **Just Give Me Bridges!** 'ı tıklayın
- *Captcha*'yı girin ve press 'a basın

*Captcha'yı doğru bir şekilde girdiğinizde **Köprü** adresleri size verilecek.*

## Bridges

*Şekil 13: Tor Projesi websitesinden alınmış Köprü adresleri*

**Not:** Köprü Veri Tabanı birilerinin tüm köprü adreslerini kolayca öğrenmesini engellemek üzere tasarlanmıştır. İlk başta size her seferinde aynı köprüleri veriyor gibi görünebilir. Bir süre sonra, yeni adresler sunmaya başlayacaktır.

Köprü adreslerini aldıktan sonra onları **Şekil 7: Köprü yapılandırma ekranı** veya **Şekil 11: Tor Tarayıcı seçenekleri**'nde görülen pencerelerdeki alanlara yapıştırın.

# Tor Tarayıcı Kullanımı

- **4.0 Tor Tarayıcı Kullanımı**
- **4.1 Tor Tarayıcı'nın çalışıp çalışmadığına dair ek kontrol**
- **4.2 Yeni bir kimlik Nasıl Yaratılır?**
- **4.3 NoScript eklentisinin etkinleştirilmesi**
- **4.3 Tor Tarayıcı güncellemeleri**

## 4.0 Tor Tarayıcı Kullanımı

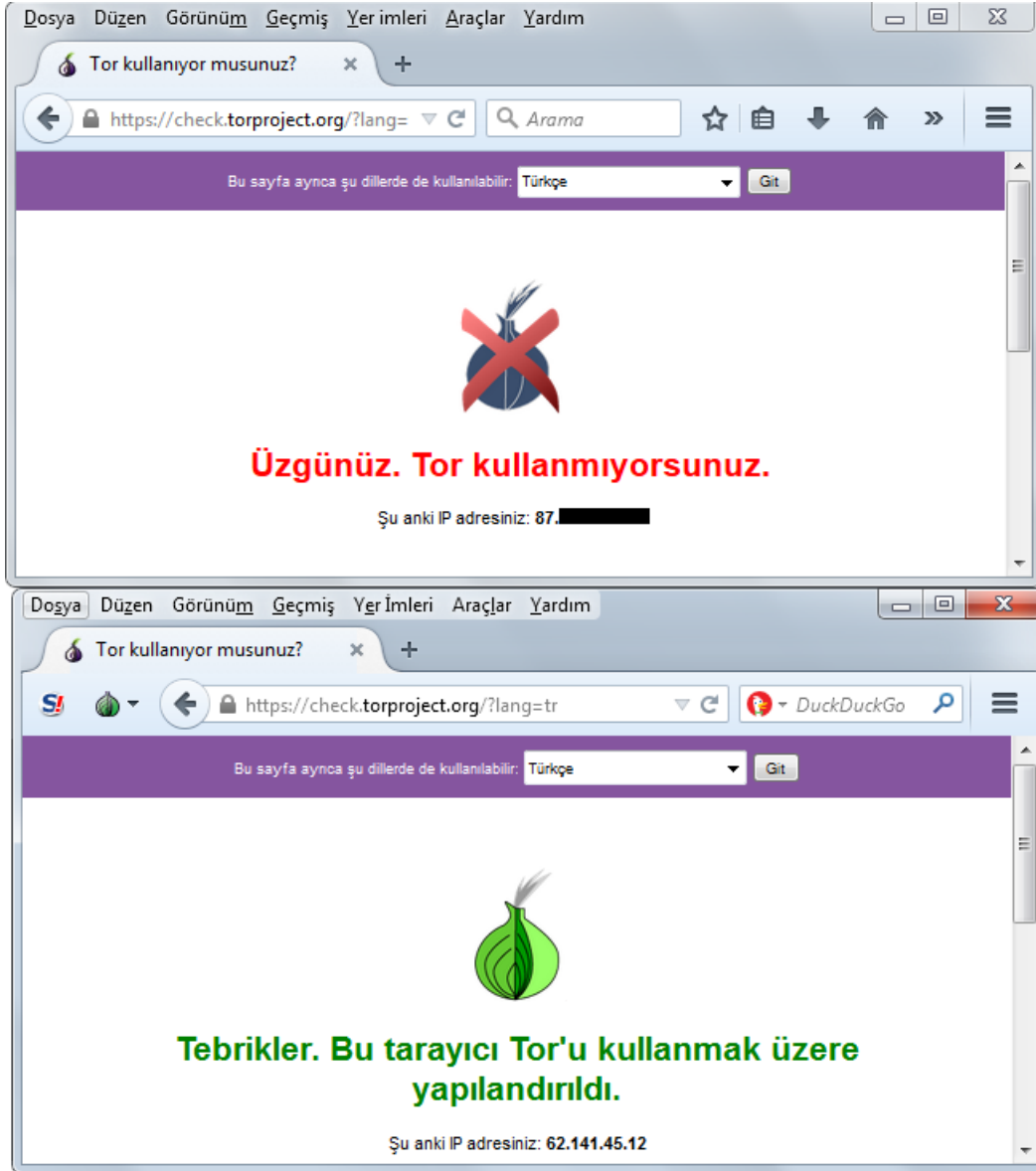
**Tor Tarayıcı** kullanımı kolay olmak üzere tasarlanmıştır. **Firefox'un** daha fazla gizlilik ve güvenlik sağlamak amacı ile değiştirilmiş bir versiyonu olduğu için, herhangi bir web tarayıcısı kullanmayı biliyorsanız, **Tor Tarayıcı'yı** kullanmanız oldukça kolay olacaktır.

**Not:** Tor Tarayıcı gizlilik amaçlı tasarlandığı için, hard diskinize veya USB çubuğuna bilgi kaydetmemek üzere yapılandırılmıştır. Bu şu anlama gelir, Tor Tarayıcı'ndan çıktığınız zaman tüm tarama tarihiniz silinir.

## 4.1 4.1 Tor Tarayıcı'nın çalışıp çalışmadığına dair ek kontrol

Her atlatıcı yazılım için olduğu gibi, **Tor Tarayıcı'nın** iyi çalıştığından emin olmak için basit bağımsız testler yapmanızı öneririz. Bunu, siteyi ziyaret ettiğiniz IP adresi üzerinden konumunuzu belirlemeye çalışan herhangi bir web sitesine giderek yapabilirsiniz.

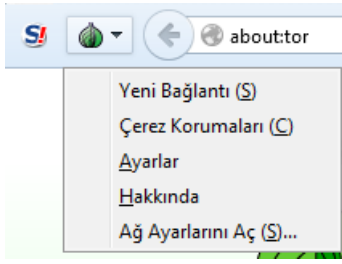
Bunu ücretsiz yapan birkaç web sitesi vardır, örneğin [check.torproject.org](https://check.torproject.org) [247], [iplocation.net](https://iplocation.net) [248], [ip2location.com](https://ip2location.com) [249], [whatismyipaddress.com](https://whatismyipaddress.com) [250]. Bu sitelere **Tor Tarayıcı** veya herhangi benzeri bir önleyici araç kullanmadan eriştiğiniz zaman gerçek IP adresinizi gösterirler ve konumunuzu aşağı yukarı doğru olan bir şekilde belirlerler. Fakat bu sitelere **Tor Tarayıcısı** veya herhangi benzeri bir atlatıcı araç kullanarak erişirseniz, konum ve IP adresinin farklı görüldüğünü göreceksiniz.



Şekil 1: Aynı bilgisayarda, Tor statüsü ve IP adres farklarını gösteren Firefox (yukarıda) ve Tor Tarayıcısı (aşağıda)

## 4.2 Yeni bir kimlik Nasıl Yaratılır?

Tarayıcınızda kullanmak üzere *yeni bir kimlik* yaratabilirsiniz. Bu demektir ki, kullanmanız için bir dizi yeni ve rastgele **Tor** proxy sunucusu seçilecektir. Bu sayede web sunucularına yeni bir konumdan ulaşıyor gibi görüneceksiniz. Bunu yapmak için 'e **tıklayın** ve menüden **Yeni Kimlik'i** seçin. **Tor Tarayıcı** kısa bir süre için kapanacak, *tarama geçmişinizi* ve *çerezlerinizi* silerek yeniden açılacaktır. Tarayıcı yeniden başladıktan sonra 4.1 bölümünde tarif edildiği gibi yeni konumunuza bakabilirsiniz.



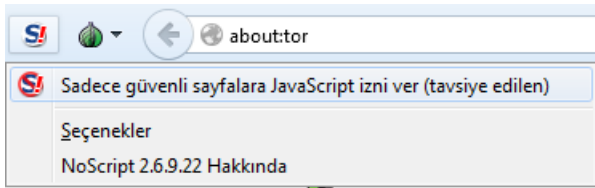
Şekil 2: TorButton menüsünden Yeni Kimlik seçimi

### 4.3 NoScript eklentisinin etkinleştirilmesi

**Tor Tarayıcı** önceden yüklenmiş **NoScript** eklentisi ile birlikte gelir. **NoScript**, **Tor Tarayıcı'da** komut çalışması yaparak zararlı web sitelerine ve gerçek kimliğinizi ifşa etmeye karşı ek koruma sağlar. Fakat, **NoScript Tor Tarayıcı'da** verili olarak devre dışı bırakılmıştır, bu yüzden de sağladığı ek koruma hemen hazır değildir.

**NoScript'in** getirdiği ek korumaları etkinleştirmek istiyorsanız, bunu **NoScript** menüsünü açıp *Global olarak Komutları Engelle*'yi tıklayarak ve sunduğu çeşitli *seçenekleri* yapılandırarak yapabilirsiniz.

**Firefox** bölümünden **NoScript** <sup>[243]</sup> hakkında daha çok bilgi edinmenizi tavsiye ederiz.



Şekil 3: Global olarak Komutları Engelle (tavsiye edilen) seçeneğini seçerek NoScript'in etkinleştirilişi

### 4.4 Tor Browser updates

**Nasıl Yapmaklı Kitapçığı 1.4 kısmında** <sup>[251]</sup> yazılımlarınızı güncellemenin ne kadar önemli olduğundan bahsetmiştik. Bu durum **Tor Tarayıcı** için de geçerlidir. Yeni bir güncelleme hazır olduğunda **Tor Tarayıcı'yı** açarken tarayıcınızın güncellenmeye ihtiyacı olduğuna dair bir uyarı alacaksınız (Şekil 4) ve *Tor Tarayıcı Güncellemesini İndir'i* tıklamanız istenecek. Bu şekilde, en son sürümüne ulaşabileceğiniz **Tor Projesi** web sitesine yönlendirileceksiniz. Son sürümü indirdikten sonra bu kılavuzu kullanarak güncellenmiş Tor Tarayıcı'yı kurabilirsiniz.



Şekil 4: Güncelleme olduğunu gösteren Tor Tarayıcı

## Tor Tarayıcı - Sıkça Sorulan Sorular

- [5.0 Sıkça Sorulan Sorular](#)
- [5.1 Ek Kaynaklar](#)

## 5.0 Sıkça Sorulan Sorular

**Tor** oldukça başarılı bir şekilde bakımı yapılan ve test edilen bir yazılımdır. **Tor ağını**, dünya çapında yüz binlerce insan kullanır ve daha güvenli ve güvenilir olması için sürekli olarak çeşitli şekillerde geliştirilir. Bu bölümdeki açıklamalar karışık gibi görünse de çoğu zaman **Tor Tarayıcı'yı** çalıştırmak için **3.1.1 Tor Ağına Nasıl Bağlanılır? Direkt Erişim bölümünü** <sup>[252]</sup> okumanıza gerek bile kalmaz.

**Soru:** Tor Tarayıcı'yı Neden Kullanmalıyım?

**Cevap:** İyi soru. Belli siteleri erişimdeki İnternet sansürünü aşmak istiyorsanız **Tor Tarayıcı** çok iyi bir araçtır. İnternet Servis Sağlayıcınızın (ISP) hangi sitelerde dolaştığınızı bilmesini istemiyorsanız veya bu sitelerin sizin konum be başlangıç noktanızı bilmesini istemiyorsanız **Tor Tarayıcı** kullanmak oldukça faydalıdır. .

**Soru:** Tor Tarayıcı'yı başlattığım zaman, diğer bütün programlarım **Tor ağı** üzerinden anonim olarak mı bağlantı kurar?

**Cevap:** Hayır, **Tor ağına** sadece **Tor Tarayıcı'dan** erişmeniz gerektiğini unutmanız gerekir. Diğer bütün programlarınız İnternet üzerindeki sunucular ile direkt olarak bağlantı kurar. **Tor ağı** üzerinden bağlantı kurduğunuzdan emin olmak için, **https://check.torproject.org** sitesini ziyaret edebilirsiniz. **Tor**, aynı zamanda, yeni ve daha önceden ziyaret etmediğiniz web siteleri hakkında sizin temkin, sağduyu ve yargılama gücünüze dayanır.

**Soru:** Tor, Tor Tarayıcı kullanarak tüm iletişimleri koruma altına alır mı?

**Cevap:** **Tor**, sizinle **Tor ağı** arasındaki ve **Tor ağı** içerisindeki tüm iletişimleri şifreler. Fakat, unutmayın ki, **Tor**, **Tor ağı** ve bağlantı kurduğunuz siteler arasındaki trafiği şifreleyemez. Bunun için **HTTPS protokolü** veya benzer başka şifreleme yöntemleri kullanmalısınız, özellikle de bilgilerinizin gizlilik ve güvenliği önemliyse!

## 5.1 Ek Kaynaklar

- [Tor Projesi](#) <sup>[253]</sup> ek destek ihtiyacında olan insanlar için (e-posta, IRC, Telefon ve benzeri yöntemler ile) [destek servisi](#) <sup>[254]</sup> sağlar.
- Resmi [Tor Sıkça Sorulan Sorular Sayfası](#) <sup>[255]</sup>.

## Sosyal Ağ Araçları: Facebook, Twitter ve Diğerleri

### Short Description:

Bu bölüm bazı popüler sosyal ağ sitelerindeki gizlilik ve güvenlik ayarları ile ilgilidir ve bu ağların kullanımını *daha güvenli*, ya da daha doğru bir ifadeyle, *daha az güvensiz* hale getirmeyi amaçlar. Facebook ve Twitter için adım adım giden bir kılavuz sağlar ve YouTube ve Flickr kullanımına yönelik genel bilgiler verir.

Bu sosyal ağ siteleri en popüler ve en sık kullanılan sosyal ağ araçlarıdır. Bu ağlara sahip olan özel şirketlerdir ve 9. Bölüm olan Sosyal ağları kullanırken kendinizi ve verilerinizi nasıl korunursunuz?'da <sup>[256]</sup> söylendiği gibi, bu şirketler kullanıcılar hakkında bilgi toplayıp bu bilgileri reklamcılara satarak para kazanırlar.

Hükümetlerin getirdiği yasaklar öncelikle bu siteleri hedef alır ve onlara erişimi engellerler. Şirketler, hükümetlerin baskısına dayanamayıp gerektiği zaman sansür uygulamalarına gidebilir. Erişim engellenmemiş olsa bile, birçok hükümet bu siteleri denetim altında tutar, kullanıcıların metaverilerin toplar ve genellikle insan hakları savunucularını da kapsayacak bir şekilde, ilgilendikleri kişilerin özel bilgilerini ister. Bu anlamda, aklınızda tutmalısınız ki, sosyal ağ sunucularını yöneten şirketler, özel datalarınız ve parolanız dahil, **tüm bilgilerinize** sahiptir.

Dijital güvenliği önemseyen aktivist bir perspektif ile yaratılmış, [Diaspora](#) <sup>[257]</sup>, [Crabgrass](#) <sup>[258]</sup>, [Friendica](#) <sup>[259]</sup>, [Pidder](#) <sup>[260]</sup>, ya da [SecureShare](#) <sup>[261]</sup> gibi alternatif sitelere bakabilirsiniz. [Social Swarm](#) <sup>[262]</sup>, tartışmalar ve sosyal ağlardaki gizlilik ile ilgili bilinç yükseltme kampanyaları yürüten, bir yandan da verimli bir öğrenme kaynağı olabilen, kar amacı gütmeyen bir organizasyon tarafından yönetilen bir beyin takımıdır.

Başka bölgelerde başka siteler popüler olabilir, bu yüzden başka seçenekleri de gözden geçirebilirsiniz. Birini seçmeden önce aşağıdaki noktaları göz önünde bulundurmalısınız:

1. **SSL** (https gibi) üzerinden bağlantıyı sadece giriş aşamasında mı, yoksa sitenin tüm kullanımları için mi sağlıyor? Şifreleme sertifikaları benzeri şifreleme problemleri var mı?
2. Son Kullanıcı Lisans Anlaşması, Gizlilik Politikası ve Veri Kullanma Politikası'nı dikkatle okuyunuz. İçeriğiniz ve kişisel verileriniz nasıl kullanılıyor? Kimlerle paylaşılıyor? Kullanıcıların birçok popüler sitenin Hizmet Kullanım Şartlarını anlamaları için faydalı eklentiler için **Terms of Service; Didn't Read'e** <sup>[263]</sup> bakınız.
3. Kullanıcılar için hangi gizlilik seçenekleri sağlanmış? Videolarınızı küçük bir grup insan ile güvenli bir şekilde paylaşabiliyor musunuz, yoksa verili olarak kamuya açık durumdalar mı?
4. **Sunucuların coğrafi konumunu**, hangi yerel hukuk sistemlerine bağlı olduğunu ve şirketlerin nereye kayıtlı olduğunu biliyor musunuz? Bu bilgilerin sizin e-posta aktivite ve bilgilerinizin gizlilik ve güvenliği bakımından ne anlama geldiğinden haberdar mısınız? Sitenin sahibi olan kimseler, herhangi bir hükümetten istek geldiği takdirde bilgilerinizi paylaşır mı?

# Facebook Güvenlik Rehberi



**Facebook** popüler bir sosyal ağ websitesidir ve neredeyse evrensel olan erişilebilirliği onun gizlilik ayarları bilgilerinin ve kontrolünün ne kadar önemli olduğunu gösterir.

## Ana Sayfa

- [www.facebook.com.tr](http://www.facebook.com.tr) <sup>[264]</sup>

## Bilgisayar Gereksinimleri

- İnternet bağlantısı
- Güvenlik eklentileri olan **Firefox web tarayıcısı** <sup>[86]</sup> **Tor Tarayıcı** <sup>[192]</sup>

## Bu bölümün son güncellenme tarihi

- Temmuz 2014

## Gerekli Okuma

- Nasıl Yapmalı Kitapçığı'nın **9. Bölüm'ü, Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz?** <sup>[256]</sup>
- Facebook'un **Kullanım Koşulları** <sup>[265]</sup> ve **Veri Kullanma Politikası** <sup>[266]</sup>

## Buradan sağlayacağınız faydalar:

- **Facebook** kullanırken kamuya açık hale getirdiğiniz kişisel bilgilerin miktarını **azaltabilmek**.
- **Facebook'taki** profil, statü güncelleme, fotoğraf ve diğer verilerinize kimin ve ne zaman ulaşabileceğini **kontrol etme** becerisi.
- **Facebook'un** reklam ortakları ve bağlı olduğu websiteleri de dahil olmak üzere üçüncü taraflara açık hale getirdiği bilgilerinizin miktarını **azaltmak**.

## 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

**Facebook** dünyanın en popüler sosyal ağ sitesidir. İnsan hakları savunucuları tarafından, ağ kurmak, iletişim kurmak, organize olmak, çeşitli konu ve aktiviteleri görünür kılmak için yaygın bir şekilde kullanılabilir ve kullanılmaktadır. Fakat bir yandan da, hak savunucularının aktivitelerine karşı olanlar için de zengin bir bilgi kaynağı olma potansiyeli vardır. Bu yüzden de, hesap ve gizlilik ayarlarını bilmek çok önemlidir.

**Facebook**, ABD başta olmak üzere, birçok hükümet tarafından aktif olarak denetlenir. Buna ek olarak, **Facebook** Veri Kullanma Politikası, hükümet soruşturmaları dahil olmak üzere herhangi bir yasal talep olduğunda bilgilerinizi paylaşacağını belirtir. **Facebook'un** açık doğası nedeniyle, sizin güvenlik ve gizliliğiniz arkadaşlarınızın ve iletişim halinde olduğunuz kimselerinkine sıkı sıkıya bağlı olduğunu unutmamak gerekir. Bu kılavuzları takip etmek size daha fazla gizlilik ve güvenlik sağlayacaktır, fakat **Facebook** arkadaşlarınızın bunları uygulamaması halinde çok da verimli olmayacaktır. Bu yüzden, bu bilgileri arkadaşlarınız, aileniz ve diğer **Facebook** temaslarınız arasında yaymanız kendinizin olduğu kadar, onların da güvenliğini sağlamak için önemlidir.

Birçok insan, sosyal, politik ve profesyonel iletişim ve organizasyon için **Facebook Grupları'nı** kullanır. Facebook size 'gizli' bir grup kurma olanağı verse de, akılda tutulmalıdır ki böyle gruplarda paylaşılan bilgiler, sadece üyeler ile değil Facebook ve talepte bulunan devlet daireleri ve diğer üçüncü taraflar dahil olmak üzere Facebook verilerine erişimi olan herkes ile de paylaşılır. Facebook'a alternatif olarak **RiseUp.Net** tarafından sağlanan **Crabgrass** servisini öneririz. Belirtmek gerekir ki, **Crabgrass** spesifik olarak aktivizm için dizayn edilmiştir. Daha fazla bilgi için, Uygulamalı Rehber: **Crabgrass Güvenli Çevrimiçi İşbirliği Platformu** <sup>[258]</sup>.

**Facebook Gizlilik Ayarları** konusunda her zaman bilgilerinizi güncellemelisiniz. Bu rehberde verilecek olan ayarlar (Haziran 2014) Facebook hesabınızı daha güvenli kılmanızı sağlayacaktır. Fakat, Gizlilik ve Güvenlik ayarlarındaki güncellemeleri ve sorularınızın cevapları için resmi **Facebook yardım sayfasına** <sup>[267]</sup> bakmanızı öneririz.

## Genel Ayarlar ve Güvenlik Ayarları

List of sections on this page:

- [2.0 Nasıl Facebook Hesabı Açılır?](#)
- [2.1 Genel Ayarlar](#)
- [2.2 Facebook Güvenlik Ayarları](#)

## 2.0 Nasıl Facebook Hesabı Açılır?

**Facebook** hesabı açmak için web tarayıcınızı açın (**Firefox web tarayıcısı** [86] veya **Tor Tarayıcı** [192] kullanmanızı öneririz) ve **Facebook** ana sayfasına gitmek için adres çubuğuna **https://www.facebook.com** yazın. https adresindeki ek s (Güvenli Soket Katmanı – SSL olarak da bilinir), güvenli ve şifrelenmiş bir bağlantı üzerinden iletişime geçtiğinizi gösterir.

**1. Adım.** İsim ve **Soyadı** alanlarını doldurun, **e-posta adresinizi** iki kere girin ve yeni bir **parola** yaratın. Ek olarak, **doğum** **günü**nüz ve **cinsiyetiniz** (sadece kadın ve erkek seçenekleri verilmiş olmasına rağmen) istenecektir.



**Kaydol**

Ücretsizdir ve her zaman ücretsiz kalacaktır.

Hakan Denemeci

hakan.denemeci@riseup.net

hakan.denemeci@riseup.net

.....

Doğum Tarihi

1 Oca 1981 Doğum tarihimizi vermem neden gerekiyor?

☐ Kadın ☒ Erkek

Kaydol düğmesine tıklayarak, Çerez Kullanımı dahil Veri İlkemizi okuduğunuzu ve Koşullarımızı kabul etmiş olursunuz.

**Kaydol**

Şekil 2: Doldurulmuş bir form

**Not: Facebook** ile kullanmak üzere yeni bir e-posta adresi almanızı öneririz. Kamuya açık veya iş e-posta adresinizi kullanırsanız karşı tarafın sizi bulması çok daha kolay olacaktır. **Facebook** Kullanım Şartları, **Facebook** kullanırken gerçek isminizi kullanmanızı ister. Bu tabii ki, karşı tarafın sizi bulmasını ve aktivitelerinizi takip etmesini kolaylaştırır. Takma bir isim kullanabilirsiniz ama bunun **Facebook** Kullanım Şartlarına aykırı olduğunu ve buna rağmen, başka kaynakların yanı sıra IP adresinizden bulunabilir olduğunuzu unutmayın. **Tor Browser** [268] gibi yazılımlar üzerinden **Facebook'a** bağlanmak da zordur, çünkü **Facebook** konumunuzu hatırlar ve sizin yaptığınız girişleri başkaları sizin hesabınıza girmeye çalışıyor şeklinde yorumlayabilir.

Tüm bunları göz önünde bulundurduğunuz zaman, bulunma ihtimalinizin ya da **Facebook** aktivitelerinizin çevrimdışı işleriniz veya kişisel hayatınız ile ilişkilendirilmesi olasılığının hayatınıza, sağlığınıza veya aile ve arkadaşlarınızın sağlığına tehdit oluşturacağını düşünüyorsanız, **Facebook** kullanmaya başlamamak iyi bir fikir olabilir. Çevrimiçi anonim kalmanın yolları üzerine **İnternette Nasıl Anonim Kalınır ve İnternet Sansürü Nasıl Aşılır?** [75] kısmına bakın.

**Not:** Hesabınızı ve bilgilerinizi korumak için güçlü bir şifre seçmenizin çok önemli olduğunu unutmayınız. Lütfen **3. Bölüm Güvenli Şifreler Nasıl Oluşturulur ve Muhafaza Edilir?** [4]'e bakın.

**2. Adım.** *Kaydol'a* tıklamadan önce **Facebook Kullanım Şartları** [265] ve **Veri Kullanma Politikası'nı** [266] okuduğunuzdan emin olun. Bunlar, **Facebook'a** hangi bilgileri verdiğiniz ve bu bilgilerin onlar tarafından nasıl kullanılacağı konusunda önemli bilgiler içerir.

**3. Adım.** *Arkadaşların Zaten Facebook'ta mı?* ekranında, **Facebook** sizin **Facebook'taki** e-posta hesabınızdan arkadaş bulabilmek ve daha sonra onları ekleyebilmeniz için e-posta hesabınızı ve parolanızı vermenizi ister. *Bu adımı atlamaz* şiddetle tavsiye ederiz.

### Arkadaşların zaten Facebook'ta mı?

Arkadaşlarının çoğu zaten burada olabilir. Arkadaşlarını Facebook'ta bulmanın en hızlı yolu e-posta hesaplarında arama yapmaktır. Nasıl çalıştığını gör.



Windows Live Messenger

MSN Kimliği

(e\_posta\_adresin@ornek.com)

[Arkadaşlarını Bul](#)

[Nasıl çalıştığını gör](#)



Outlook.com (Hotmail)

[Arkadaşlarını Bul](#)



Yahoo!

[Arkadaşlarını Bul](#)



Diğer E-posta Hizmeti

[Arkadaşlarını Bul](#)

[Bu adımı geç](#)

Şekil 3: Arkadaşlarınızı Bulun ekranı

**4. Adım. Profil Bilgileri** ekranında **Facebook**, gitmiş olduğunuz Lise, Kolej veya Üniversite veya iş yeriniz gibi bilgileri girmenizi ister. Bu bilgiler arkadaşlarınızın sizi bulmasını kolaylaştırır da karşı tarafların da sizi bulmasını kolaylaştırır. *Bu adımı atla'yı tıklayarak* geçmenizi öneririz.

Bu adımda vereceğiniz bilgilere dayanarak **Facebook** size, arkadaş olarak eklemek isteyebileceğiniz olası sınıf arkadaşlarınız veya meslektaşlarınız konusunda önerilerde bulunur. Bu aşamada da, kimleri eklemek istediğinizi dikkatlice düşünün ve **tanımadığınız ve güvenmediğiniz kişileri eklemeyin**.

Bu aşamada herhangi bir arkadaş eklemek istemiyorsanız *bu adımı da atlayabilirsiniz*.

### Fill out your profile info

This information will help you find your friends on Facebook.

Current City



Hometown



High School



College/University



Employer



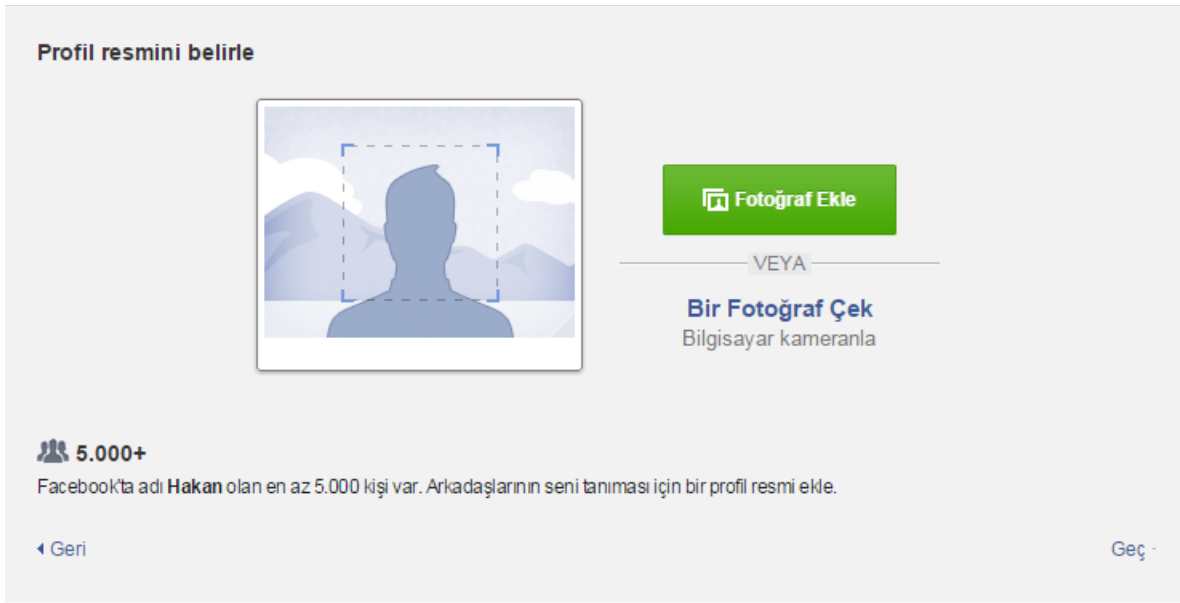
[Back](#)

[Skip](#)

[Next](#)

Şekil 4: Profil Bilgisi ekranı

**5. Adım. Profil resmini belirle** ekranında **Facebook** sizden, **yükleyerek** ya da web kamerası ile bir fotoğraf **çekerek**, kendi fotoğrafınızı eklemenizi ister.



Şekil 5: Profil resmini belirle ekranı

Not: Bu fotoğraf, **Facebook** zaman tünelineki *kapak fotoğrafınız* ile birlikte, **profilinize giren herkese, arkadaşınız olmasalar dahi** ve gizlilik ayarlarınızdan bağımsız olarak, görünür olacaktır. Kendinizin, arkadaşlarınızın, meslektaşlarınızın ve organizasyonunuzun karşı taraflarca tanınabileceği bir fotoğraf kullanmak isteyip istemediğinizi dikkatlice düşünün.

*Atla* veya *Kaydet ve Devam Et'i tıkladığınız* zaman, sağladığınız e-posta adresinin gelen kutusuna yönlendirileceksiniz. Burada, **Facebook** tarafından gönderilmiş e-posta adresinizin geçerliliğini onaylamanızı isteyen bir e-posta bulacaksınız. Bunu yaptığınız zaman, **Facebook** sayfanız hazır hale gelecektir.

## 2.1 Genel Ayarlar

**6. Adım. Facebook** ana sayfanızdan, *Ana Sayfa'nın* yanındaki küçük oka **tıklayıp Ayarlar'ı** seçin.



Şekil 6: Seçenekler

Bu sizi **Ayarlar** menüsüne yönlendirecek. Sol taraftan farklı ayar kategorileri seçebilirsiniz. İlk sekme, isminiz, soyadınız, e-postanız, şifreniz, ağlarınız ve kullanacağınız dil konularında ayarlamalar yapabileceğiniz *Genel Hesap Ayarları* olacak.

Genel

Güvenlik

Gizlilik

Zaman Tüneli ve Etiketleri...

Engelleme

Bildirimler

Mobil

Takipçiler

Uygulamalar

Reklamlar

Ödemeler

Destek Panosu

Videoalar

### Genel Hesap Ayarları

|               |                                         |         |
|---------------|-----------------------------------------|---------|
| Adın          | Grens Edelstaal                         | Düzenle |
| Kullanıcı Adı | http://www.facebook.com/grens.edelstaal | Düzenle |
| E-posta       | Ana: shockingblue23@hotmail.com         | Düzenle |
| Şifre         | Şifre daha önce hiç değiştirilmedi.     | Düzenle |
| Ağlar         | Ağ yok.                                 | Düzenle |
| Dil           | Türkçe                                  | Düzenle |
| Sıcaklık      | Santigrat                               | Düzenle |

Facebook verilerinin kopyasını indir.

Şekil 7: Genel Hesap Ayarları

**7. Adım.** Şifrenizi, tercihen üç ayda bir olmak üzere, düzenli olarak **güncellemenisiniz**. Hesabınızı ve bilgilerinizi korumak için güçlü bir şifre seçmenizin çok önemli olduğunu aklınızdan çıkarmayın. Lütfen Kullanma Kılavuzundaki **3. Bölüm Güvenli Şifreler Nasıl Oluşturulur ve Muhafaza Edilir?** [4]'e bakınız.

Şifre

Mevcut

Yeni

Şifre güvenliği: Güçlü

Yeni şifreyi tekrar yaz

Şifreler aynı

Değişiklikleri Kaydet

İptal

Şekil 9: Şifre seçenekleri

**8. Adım.** Ağlarınız: **Facebook**, lise, üniversite, işverenin, oturduğunuz yer veya şehir üzerinden çeşitli ağlara katılmanıza olanak verir ve bu sayede insanların size daha kolay ulaşmasını sağlar. Bu sizin de insanları daha kolay bulmanızı sağlayacak olsa da, istemediğiniz kimselerin de sizi bulmasını kolaylaştırır. Bu siteyi kullanan insanların sayısı göz önünde bulundurulduğu zaman, bildiğiniz ve güvendiğiniz insanlarla **Facebook** üzerinden iletişim kurmanız için ağlara katılmanızın gerekeceği ortadadır.

## 2.2 Facebook Güvenlik Ayarları

**9. Adım.** Menünün solundaki **Güvenlik** tıklayın. Bu Güvenlik Ayarları sayfasını açacak.

### Güvenlik Ayarları

|                                |                                                                                                                        |         |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------|---------|
| Giriş Uyarıları                | Herhangi biri yeni bir cihazdan veya tarayıcıdan senin hesabına giriş yaptığında uyarı al.                             | Düzenle |
| Giriş Onayları                 | Hesabına başka insanların giriş yapmasını önlemek için telefonunu ilave bir güvenlik önlemi olarak kullan.             | Düzenle |
| Kodmatik                       | Gerektiğinde güvenlik kodları almak için Facebook uygulamasını kullan.                                                 | Düzenle |
| Uygulama Şifreleri             | Uygulamalarına giriş yapmak için Facebook şifreni veya Giriş Onayları kodlarını kullanmak yerine özel şifreler kullan. | Düzenle |
| Güvenilir Kişiler              | Hesabın kilitlenirse hesabına tekrar erişmene yardımcı olmaları için arayabileceğin arkadaşlarını seç.                 | Düzenle |
| Tarayıcıların ve Uygulamaların | Hangi tarayıcıları sık kullandığın tarayıcılar olarak kaydettiğini gözden geçir.                                       | Düzenle |
| Giriş Yaptığın Yer             | Şu anda Facebook'a giriş yapmış olduğun yeri gözden geçir ve yönet.                                                    | Düzenle |

Hesabını dondur.

Şekil 10: Güvenlik Ayarları sayfası

**10. Adım.** Giriş Uyarıları sekmesine tıklayın. Buradan, **Facebook** sayfanıza daha önce kullanmadığınız bir araçtan giriş yapılması halinde bildirim gönderilmesini isteyebilirsiniz. Uyarıları E-posta ya da Metin İletisi/Anlık Bildirim yoluyla almak

istediğiniz yönünde tercih yapınız.

**Not:** Bildirimleri Metin İleti yoluyla almayı seçerseniz, telefon numaranızı **Facebook** hesabınıza bağlamanız gerekir ki bu da site üzerindeki aktivitelerinizi daha kolay teşhis edilebilir duruma getirir.

**Giriş Uyarıları**

Herhangi biri yeni bir cihazdan veya tarayıcıdan senin hesabına giriş yaptığında uyarı al.

**Bildirimler**

☐ Bildirimler al

☒ Bildirimler alma

**E-posta**

☐ Giriş uyarılarını hakan.denemeci@riseup.net adresine gönder

☒ E-posta uyarıları alma

**Kısa mesajlar**

☐ Telefon numaranı bağla

☒ Kısa mesaj uyarıları alma

[Değişiklikleri Kaydet](#) [İptal](#)

Şekil 12: Giriş Uyarıları Seçenekleri

**11. Adım. Giriş Onayları:** Ek güvenlik için, **Facebook'un** tanımadığı herhangi bir bilgisayar ya da araç üzerinden hesabınıza erişildiği her seferde güvenlik kodu girmeyi tercih edebilirsiniz. Güvenlik kodu mesaj olarak cep telefonunuza gönderilecektir..

**Not:** Bu seçeneği etkinleştirmek cep telefonunuza erişimi olmayan birisinin hesabınıza erişmesini zorlaştırır. Fakat, yukarıda da söylendiği üzere, cep telefonu numaranızı Facebook hesabınıza bağlamanızı da gerektirir. Kendi şartlarınızla göre bu durumun avantaj ve dezavantajlarını gözden geçirerek hangi tercihin sizin için daha güvenli olduğu sonucuna varabilirsiniz.

**Giriş Onayları**

☐ Bilinmeyen tarayıcılardan hesabıma erişmek için güvenlik kodu istensin [?]

[Değişiklikleri Kaydet](#) [İptal](#)

Şekil 13: Giriş Onayları seçenekleri

**12. Adım. Kodmatik:** Bu ayar, giriş kodları ve yeni şifre üretmek için akıllı telefonunuzda **Facebook** telefon uygulaması kullanmanızı sağlar.

**Kodmatik**

Facebook mobil uygulamadaki Kodmatik'i şifreni yenilemek veya Giriş Onayları güvenlik kodları oluşturmak için kullanabilirsin.

Android veya iOS cihazındaki Facebook uygulamasında Kodmatik'i Etkinleştir.

Güvenlik kodları almak için başka bir şekilde kur.

[Kapat](#)

**13. Adım. Uygulama Parolaları:** **Facebook'ta** uygulama kullanıyorsanız, bu seçenek onlar için kişisel parola oluşturmanızı sağlar. Fakat, herhangi özel bir sebebiniz yoksa Facebook uygulamasından uzak durmanızı öneririz.

**Uygulama Şifreleri**

Daha fazla bilgi al uygulama şifreleri hakkında. [Uygulama şifreleri oluştur](#)

[Değişiklikleri Kaydet](#) [İptal](#)

**14. Adım. Güvenilir Kişiler:** Bu seçenek, herhangi bir sebepten dolayı hesabınıza giriş yapamadığınız durumlarda **Facebook** arkadaşlarınız arasından seçeceğiniz kontakların size yardım edebilmesini sağlar. Bu, o kişilerle gizli bir kodu paylaşmanızı gerektirir. Bu seçeneği kullanacaksanız, güvendiğiniz kimseleri seçmek konusunda dikkatli olmanızı ve kodu paylaşırken güvenli bir iletişim <sup>[269]</sup> kurmanızı tavsiye ederiz.

**Güvenilir Kişiler**

Güvenilir kişiler, hesabına erişmekte güçlük çekmen durumunda sana güvenli bir şekilde yardımcı olabilecek arkadaşlardır.

Henüz hiç güvenilir kişi seçmedin. Güvenilir kişileri seç.

Kapat

**15. Adım. Güvenilen Tarayıcılar:** Buradan, **Facebook** hesabınıza erişim için kullanabileceğiniz tarayıcıları gözden geçirebilirsiniz.

**16. Adım. Giriş Yaptığınız Yer:** Bu, çıkış yapmayı unuttuğunuz (internet kafe veya bir arkadaşın bilgisayarında) ve hala etkin olan **Facebook** oturumlarının ayrıntılarını gösterir. Konumlar IP adresleri tarafından belirlenir.

**Giriş Yaptığınız Yer**

| Mevcut Oturum |                                          |
|---------------|------------------------------------------|
| Konum         | Amsterdam, Netherlands (Yaklaşık olarak) |
| Cihaz Türü    | Windows 7 üzerinde Chrome                |

Kapat

Şekil 14: Giriş Yaptığınız Yer listesi örneği..

Başka birisinin **Facebook** hesabınıza erişimini engellemek için bu oturumları kapatmak çok önemlidir, özellikle de listede sizin olmayan veya tanımadığınız araçlar olduğunu görüyorsanız. Bu oturumları kapatmak için, etkin oturumun yanındaki **Oturumu Bitir**'i tıklayın.

## Gizlilik ve Zaman Tüneli Ayarları

Bu sayfadaki kısımların listesi:

- [3.1 Gizlilik Ayarları ve Araçları](#)
- [3.2 Zaman Tüneli ve Etiketleme](#)
- [3.3 Kullanıcı ve Uygulamaları Engelleme](#)
- [3.4 Takipçiler](#)

### 3.1 Gizlilik Ayarları ve Araçları

**1. Adım. Facebook** *Gizlilik Ayarlarınızı* düzenlemek için, üst sağ köşede, *Ana Sayfa'nın* yanındaki küçük oka basıp *Ayarlar*'ı seçin.

 **Hakan**  

[Sayfa Oluştur](#)

[Reklam Oluştur](#)

[Facebook'ta Reklam Verme](#)

[Hareketler Dökümü](#)

[Haber Kaynağı Tercihleri](#)

[Ayarlar](#)

[Çıkış Yap](#)

[Yardım](#)

[Sorun Bildir](#)

Figure 1: Options

**2. Adım.** Bu sizi *Ayarlar* menüsüne yönltecek. Sol kısımdaki *Gizlilik*'i seçin.

## Gizlilik Ayarları ve Araçları

|                                    |                                                                                                       |                            |                            |
|------------------------------------|-------------------------------------------------------------------------------------------------------|----------------------------|----------------------------|
| Paylaştıklarımı kimler görebilir?  | İleride paylaşacağın gönderileri kimler görebilir?                                                    | Arkadaşlar                 | Düzenle                    |
|                                    | Tüm gönderilerini ve etiketlenmiş olduğu şeyleri gözden geçir                                         |                            | Hareketler Dökümünü Kullan |
|                                    | Arkadaşlarının arkadaşlarıyla veya Herkese Açık paylaşmış olduğu gönderilerin hedef kitlesini sınırla |                            | Geçmiş Gönderileri Sınırla |
| Benimle kimler iletişim kurabilir? | Sana kimler arkadaşlık isteği gönderebilir?                                                           | Herkese                    | Düzenle                    |
|                                    | Kimlerin mesajlarının Gelen Kutuma düşmesini istiyorum?                                               | Temel Filtreleme           | Düzenle                    |
| Aramada beni kimler bulabilir?     | Facebook'ta kayıtlı e-posta adresini aratarak seni kimler bulabilir?                                  | Arkadaşlarının Arkadaşları | Düzenle                    |
|                                    | Facebook'ta kayıtlı telefon numaranı aratarak seni kimler bulabilir?                                  | Arkadaşlarının Arkadaşları | Düzenle                    |
|                                    | Diğer arama motorlarının zaman tüneline bağlantı vermesini istiyor musun?                             | Hayır                      | Düzenle                    |

Şekil 2: Gizlilik ayarları sayfası

### İçeriğimi kim görebilir?

**3. Adım.** Buradaki ilk seçenek gelecek statü güncellemeleriniz için verili bir kural koymaktır: *Gelecekteki gönderilerinizi kim görebilir?* Bu gönderileri herkese, **Facebook** arkadaşlarınıza, sadece kendinize veya belirleyeceğiniz bir grup insana erişilebilir **kılabilirsiniz**. İstedığınız takdirde, bu ayarları her gönderi için değiştirebilir, bazılarını herkese, bazılarını ise arkadaşlarınıza ya da belirli bir gruba açık hale getirebilirsiniz. Unutmayın ki **Facebook'a** gönderdiğiniz tüm iletiler (Sadece Ben seçeneğini seçtiğiniz halde bile) Facebook tarafından kaydedilir ve üçüncü taraflara iletilir.

**4. Adım.** İkinci seçenek, diğer **Facebook** kullanıcılarının sizi etiketlediği gönderileri **gözden geçirmenizi** sağlar. Bunu yapmak için *Etkinlik Günlüğü Kullan'ı* tıklayın.

Paylaştıklarımı kimler görebilir?

İleride paylaşacağın gönderileri kimler görebilir?

Kapat

Paylaştığın şeylerin gizliliğini **paylaşım**da bulunurken hedef kitle seçiciyi kullanarak yönetebilirsin. Bu kontrol, seçimini hatırlar ve böylece gelecekteki gönderilerin hedef kitleyi değiştirmedğin sürece aynı hedef kitleyle paylaşılır.

Ne düşünüyorsun?

Arkadaşlar ▼

Paylaş

Tüm gönderilerini ve etiketlenmiş olduğu şeyleri gözden geçir

Hareketler Dökümünü Kullan

Arkadaşlarının arkadaşlarıyla veya Herkese Açık paylaşmış olduğu gönderilerin hedef kitlesini sınırla

Geçmiş Gönderileri Sınırla

Şekil 3: Gelecekteki gönderilerinizi kim görebilir?

**5. Adım.** Üçüncü seçenek, daha önceden halka açtığınız statü güncellemelerinizi **sınırlandırmanızı** sağlar. **Fakat**, etiketlediğiniz kimseler ve onların arkadaşları bu gönderileri görebilmeye devam eder.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                    |                            |         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|----------------------------|---------|
| Paylaştıklarını kimler görebilir?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ileride paylaşacağın gönderileri kimler görebilir? | Arkadaşlar                 | Düzenle |
| Tüm gönderilerini ve etiketlenmiş olduğu şeyleri gözden geçir                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                    | Hareketler Dökümünü Kullan |         |
| <b>Zaman Tünelindeki Eski Gönderilerin Hedef Kitlelerini Sınırla</b> <span>Kapat</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                    |                            |         |
| <p> Bu aracı kullanırsan, zaman tünelinde arkadaşlarının arkadaşları ile veya herkese açık paylaştığın içeriklerin gizlilik ayarı Arkadaşlar'a değişecektir. Hatırlatma: Etiketlenen kişiler ile bu kişilerin arkadaşları bu gönderileri görebilecektir.</p> <p>Ayrıca gönderilerinin her birinin kendi hedef kitlelerini belirleyebilirsin. Tek yapman gereken, değiştirmek istediğin gönderiye gidip farklı bir hedef kitle seçmektir.</p> <p><a href="#">Etki gönderileri nasıl değiştirebileceğini öğren</a></p> <p><span>Eski Gönderileri Sınırla</span></p> |                                                    |                            |         |

Şekil 4: Önceki gönderileri sınırlandır

#### Kim benimle temas kurabilir?

**6. Adım.** Bu kısımda size kimlerin arkadaşlık teklifi gönderebileceğine karar verebilirsiniz. Bu konu bilgi güvenliği açısından çok da önemli değildir, çünkü bu teklifleri kabul edip etmemek sizin ellinizdedir ve siz de bilmediğiniz veya tanımadığınız insanları eklememek konusunda çok dikkatli olmalısınız. Bu ayarları değiştirmek istiyorsanız *Düzenle*'yi **tıklayın**.

**7. Adım. Gelen kutuma gelen mesajları nasıl filtreleyebilirim?:** Facebook aldığınız mesajları iki klasöre koymanıza izin verir: *Gelen Kutusu* ve *Diğer*. Buradan, arkadaş listenizde olmayan insanların mesajlarını daha kolay geçiren Temel Filtreleme, veya daha zor geçiren Katı Filtreleme'yi **seçebilirsiniz**.

|                                                                                                              |                                             |         |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------|---------|
| Benimle kimler iletişim kurabilir?                                                                           | Sana kimler arkadaşlık isteği gönderebilir? | Kapat   |
| <span> Arkadaşları</span> |                                             |         |
| Kimlerin mesajlarının Gelen Kutuma düşmesini istiyorum?                                                      | Temel Filtreleme                            | Düzenle |

Şekil 5: Kimler benimle iletişim kurabilir?

#### Kimler benimle ilgili bilgilere ulaşabilir?

**8. Adım.** Buradan, telefon numaranız ve e-posta adresinizi bilen insanların sizinle ilgili bilgilere ulaşmasını zorlaştırabilirsiniz (bu teknik olarak hala mümkün olsa da). Aynı zamanda insanların arama motorları üzerinden Facebook sayfanızı bulmasını zorlaştırabilirsiniz. Verili ayarlar insanların sizi bu şekilde bulmasını olabilecek en kolay hale getirmiştir, aynı durum istemediğiniz kimseler için de geçerlidir. İlk iki seçenekte *Düzenle*'yi **tıklayın** ve e-posta adresiniz ve telefon numaranız ile sadece **arkadaşlarınız** tarafından bulunabilmeyi seçin. Üçüncü seçenek için ise, *Düzenle*'yi **tıklayın** ve *Diğer arama motorlarının zaman tünelinize link vermesine izin ver* seçeneğinin işaretini kaldırın.

|                                                                                                                                                                                                                                                                                                    |                                                                      |            |         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|------------|---------|
| Aramada beni kimler bulabilir?                                                                                                                                                                                                                                                                     | Facebook'ta kayıtlı e-posta adresini aratarak seni kimler bulabilir? | Arkadaşlar | Düzenle |
|                                                                                                                                                                                                                                                                                                    | Facebook'ta kayıtlı telefon numaranı aratarak seni kimler bulabilir? | Arkadaşlar | Düzenle |
| <b>Diğer arama motorlarının zaman tüneline bağlantı vermesini istiyor musun?</b> <span>Kapat</span>                                                                                                                                                                                                |                                                                      |            |         |
| Lütfen unutma:                                                                                                                                                                                                                                                                                     |                                                                      |            |         |
| <ul style="list-style-type: none"><li>Bu ayar açıkken, diğer arama motorlarının arama sonuçlarında zaman tüneline bağlantı vermesi daha kolaydır.</li><li>Bu ayarı kapatırsan, arama motorlarının sonuçlarında zaman tünelinin bağlantısını göstermeyi bırakmaları biraz zaman alabilir.</li></ul> |                                                                      |            |         |
| <input type="checkbox"/> Diğer arama motorlarının zaman tüneline bağlantı vermesine izin ver                                                                                                                                                                                                       |                                                                      |            |         |

Şekil 6: Kimler benimle ilgili bilgilere ulaşabilir?

## 3.2 Zaman Tüneli ve Etiketleme

Daha önce de söylediğimiz gibi, **Facebook'taki** bilgilerinizin güvenliği arkadaşlarınızın **Facebook'u** nasıl kullandığı ile çok yakından ilgilidir. *Zaman Tüneli* ve *Etiketleme* menüsünde, arkadaşlarınız sizi veya gönderilerinizi etiketlediğinde veya zaman tünelinize gönderi ekledikleri zaman neler olacağını belirleyebilirsiniz.

**1. Adım.** Sol taraftaki yan sekmedeki *Zaman Tüneli* ve *Etiketleme* menüsüne **tıklayın**.

Genel

Güvenlik

Gizlilik

Zaman Tüneli ve Etiket...

Engelleme

Bildirimler

Mobil

Takipçiler

Uygulamalar

Reklamlar

Ödemeler

Destek Panosu

Videolar

## Zaman Tüneli ve Etiketleme Ayarları

|                                                                                      |                                                                                                                |                         |         |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------|---------|
| <b>Zaman tünelime kimler bir şey ekleyebilir?</b>                                    | Zaman tünelinde kimler paylaşımda bulunabilir?                                                                 | Arkadaşlar              | Düzenle |
|                                                                                      | Arkadaşlarının seni etiketlediği gönderiler zaman tünelinde görünmeden önce onayına sunulsun mu?               | Kapalı                  | Düzenle |
| <b>Zaman tünelimdeki şeyleri kimler görebilir?</b>                                   | Diğer insanların zaman tünelinde neleri gördüğünü gözden geçir                                                 | Başkasının Gözünden Gör |         |
|                                                                                      | Etiketlendiğin gönderileri zaman tünelinde kimler görebilir?                                                   | Arkadaşlar              | Düzenle |
|                                                                                      | Başkalarının senin zaman tünelinde paylaştığı gönderileri kimler görebilir?                                    | Arkadaşlar              | Düzenle |
| <b>İnsanların eklediği etiketleri ve etiketleme önerilerini nasıl yönetebilirim?</b> | İnsanların senin gönderilerine eklediği etiketler Facebook'ta gözükmeden önce onayına sunulsun mu?             | Kapalı                  | Düzenle |
|                                                                                      | Bir gönderide etiketlendiğinde, hedef kitlede olmayan kimleri hedef kitleye eklemek istersin?                  | Arkadaşlar              | Düzenle |
|                                                                                      | Sana benzeyen fotoğraflar yüklendiğinde, etiket önerilerini kimler görür? (Bu özellik henüz sana açılmamıştır) | Kullanılmıyor           |         |

Şekil 7: Zaman Tüneli ve Etiketleme menüsü

**2. Adım.** Zaman tünelinin sadece *size* ait olmasını istiyorsanız, zaman tünelinize sizden başkasının gönderi eklemesini **engelleme**ni şiddetle tavsiye ederiz. Bunu yapmak için, *Zaman tünelime kimler gönderi ekleyebilir?* kısmında *düzenle*'yi tıklayın ve *Sadece ben*'i seçin.

**3. Adım.** Buradan, arkadaşlarınız gönderi ve fotoğraflarında sizi etiketlediği zaman ne olacağına karar verebilirsiniz. Zaman tünelinizde arkadaşlarınızdan gelecek istenmeyen etiketlemeler olmasını istemiyorsanız, *düzenle*'yi seçip *Arkadaşlarımdan beni etiketlediği gönderilere gözden geçir...* seçeneğini **etkinleştirmenizi** tavsiye ederiz. Fakat böyle yapmanız onlardan gelecek gönderilerin (ve sizi içeren etiketlemelerin) onların arkadaşlarına veya belki de halka açık ve görünür olmasını engellemez, bunu belirleyecek olan arkadaşlarınızın kendi ayarlarıdır.

|                                            |                                                                                                  |            |         |
|--------------------------------------------|--------------------------------------------------------------------------------------------------|------------|---------|
| Zaman tünelime kimler bir şey ekleyebilir? | Zaman tünelinde kimler paylaşımda bulunabilir?                                                   | Sadece Ben | Düzenle |
|                                            | Arkadaşlarının seni etiketlediği gönderiler zaman tünelinde görünmeden önce onayına sunulsun mu? | Açık       | Düzenle |

Şekil 8: Kimler zaman tünelime eklemeyebilir?

**4. Adım.** *Zaman tünelimdekileri kimler görebilir?* Bu madde bir önceki seçenekler ile ilgilidir. Bir önceki bölümde kimlerin zaman tünelinize eklemeyebileceğine karar verdiniz. Burada ise, bunları kimlerin görebileceğine dair düzenleme yapabilirsiniz. Etiketlendiğiniz gönderileri veya başkalarının zaman tünelinize yaptığı eklemeleri herkesin, arkadaşlarınızın arkadaşlarının, seçili bir grubun veya sadece kendinizin görmesi ile ilgili ayarları değiştirmek için *Düzenle*'yi **tıklayın**.

Birinci seçenek olan *Olarak Görüntüle* belli kişilerin zaman tünelinizde neler göreceğini görmenin ilginç bir yöntemidir. Fakat, aklınızda tutun ki, **Facebook** yukarıdaki tüm bilgileri kaydeder ve yasal yaptırımlar dahil olmak üzere gerektiğinde üçüncü partiler ile paylaşabilir.

|                                             |                                                                             |                         |         |
|---------------------------------------------|-----------------------------------------------------------------------------|-------------------------|---------|
| Zaman tünelimdeki şeyleri kimler görebilir? | Diğer insanların zaman tünelinde neleri gördüğünü gözden geçir              | Başkasının Gözünden Gör |         |
|                                             | Etiketlendiğin gönderileri zaman tünelinde kimler görebilir?                | Sadece Ben              | Düzenle |
|                                             | Başkalarının senin zaman tünelinde paylaştığı gönderileri kimler görebilir? | Sadece Ben              | Düzenle |

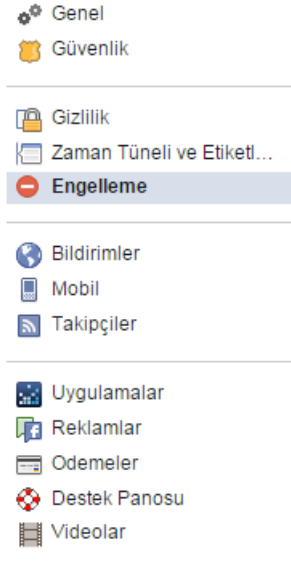
Şekil 9: Kimler zaman tünelimdekileri görebilir?

**5. Adım.** *İnsanların eklediği etiketlemeleri ve etiketleme önerilerini nasıl düzenleyebilirim?* Bu bölüm, diğer **Facebook** kullanıcılarının sizin gönderilerinize eklediği etiketlemeleri Facebook'ta

görünmeden önce gözden geçir seçeneğini **açık tutmanız** ve ikinci seçenek için **Sadece ben'i seçerek** kısıtlamanızı tavsiye ederiz. **Facebook**, arkadaşlarınızın fotoğrafları içinde size benzeyenleri tanıyan ve onlara bu fotoğraflarda sizi etiketlemesini öneren yeni bir **yüz tanıma** teknolojisi kullanmaya başladı. Doğal olarak, hak savunucuları için bu özellikle hassas bir durum olabilir, bu yüzden de bu seçeneği **devre dışı** bırakmanızı şiddetle salık veririz.

## Kullanıcıları ve Uygulamaları Engellemek

**6. Adım.** Soldaki menüden *Engelleme*'yi seçin. Burada **Facebook**, istenmeyen, ihlal edici ve bazen de potansiyel olarak tehlikeli bilgileri engellemek için çok çeşitli seçenekler sunar.



Şekil 10: Açılır listeden Engelle'yi seçin.

**7. Adım.** *Sınırlandırılmış Liste*. Buradan, **Facebook** arkadaşlarınızın sadece zaman tünelinizde halka açık olarak paylaştıklarını görmesi için bir listeye ekleyebilirsiniz (yukarıda incelediğimiz ayarlar üzerinden). Arkadaşlarınızı bu listeye eklemek için, *Listeyi Düzenle*'yi tıklayın.

|                    |                                                                                                                                                                                                                  |                 |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Kısıtlılar Listesi | Kısıtlılar listene eklediğin arkadaşlar senin sadece herkese açık yaptığın bilgilerini ve güncellemelerini görebilir. Facebook Kısıtlılar listene eklediğin arkadaşlarına bununla ilgili bir bildirim göndermez. | Listeyi Düzenle |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|

Şekil 11: Sınırlandırılmış Liste

**8. Adım.** *Kullanıcıları Engelle*. Buradan **Facebook** sayfanıza veya içeriklerinize erişen veya sizi arkadaş olarak ekleyen bir kullanıcıyı engelleyebilirsiniz.

|                       |                                                                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kullanıcıları engelle | Birini engellediğinde, bu kişi senin zaman tünelinde paylaştığın şeyleri göremez, seni etiketleyemez, seni etkinliklere veya gruplara davet edemez, seninle konuşma başlatamaz ve seni arkadaş olarak ekleyemez. Not: Buna ikinizin de katıldığınız uygulamalar, oyunlar veya gruplar dahil değildir. |
| Kullanıcıları engelle | <div><input type="text" value="Ad veya e-posta ekle"/><br/><input type="button" value="Engelle"/></div>                                                                                                                                                                                               |

Şekil 12: Kullanıcıları Engelle

**9. Adım.** *Uygulama davetlerini engelle*. Sıklıkla, oyun gibi herhangi bir uygulamaya ilgi duyan bir **Facebook** arkadaşı mevcuttur ve bu kişi oyuna katılmamız için bize düzenli olarak davet yollar. Buradan, arkadaşlarınızdan gelen bu tür uygulama davetlerini engelleyebilirsiniz.

|                                    |                                                                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Uygulama davetlerini engelle       | Birisinden uygulama davetlerini engellediğinde, o arkadaşının gelecekte göndereceği uygulama isteklerini otomatik olarak yok sayarsın. |
| Bu kişiden gelen davetleri engelle | <div><input type="text" value="Bir arkadaşının adını yaz..."/></div>                                                                   |

### Şekil 13: Uygulama Davetlerini Engelle

**10. Adım.** *Etkinlik davetlerini engelle.* Aynı şekilde, **Facebook** arkadaşlarınızdan gelen etkinlik davetlerini engelleyebilirsiniz.

|                                           |                                                                                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Etkinlik davetlerini engelle</b>       | Birisinden gelen etkinlik davetlerini engellediğinde, bu arkadaştan gelecek etkinlik isteklerini otomatik olarak yok sayarsın. |
| <b>Bu kişiden gelen davetleri engelle</b> | <input type="text" value="Bir arkadaşının adını yaz..."/>                                                                      |

### Şekil 14: Etkinlik Davetlerini Engelle

**11. Adım.** *Uygulama engelle.* İsminden da anlaşılacağı üzere, buradan, bir uygulamanın, halka açık bilgileriniz dışındaki bilgilerinize ulaşmasını engelleyebilirsiniz.

|                             |                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Uygulamaları engelle</b> | Bir uygulamayı engellediğinde, uygulama Facebook üzerinden seninle iletişim kuramaz ve senin herkese açık olmayan bilgilerini alamaz. <a href="#">Daha fazla bilgi al</a> |
| <b>Uygulamaları engelle</b> | <input type="text" value="Bir uygulamanın adını yaz..."/>                                                                                                                 |

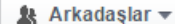
### Şekil 15: Uygulama Engelle

## 3.4 Takipçiler

**Facebook**, arkadaşınız olmayan kimselerin de haber akışınızı takip etmesine izin verir. Fakat, aklınızda tutmalısınız ki, başkalarının haber akışınızı takip etmesine izin verirseniz, verilerinizin bir bölümünün bu insanların ve onların ağında olan diğer kişilerin eline geçmesine de izin vermiş olursunuz.

**16. Adım.** Soldaki menüden *Takipçiler'i* tıklayın.

**17. Adım.** *Arkadaşlar'ın seçili* olduğundan emin olun.

|                                   |                                                                                                                                                                                                                                                                       |                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Beni Kimler Takip Edebilir</b> | Takipçiler senin gönderilerini Haber Kaynağı'nda görür. Arkadaşların, gönderilerini varsayılan olarak takip eder, ancak gönderilerini arkadaşın olmayan kişilerin de takip etmesine izin verebilirsin. Seni kimlerin takip edebileceğini seçmek için bu ayarı kullan. |  |
|                                   | Paylaşımında bulunduğun her zaman, içeriği kendileriyle paylaşmak istediğin hedef kitleyi seçebilirsin.                                                                                                                                                               |                                                                                       |
|                                   | <a href="#">Daha fazla bilgi al.</a>                                                                                                                                                                                                                                  |                                                                                       |

### Şekil 18: Takipçiler ayarları

# Uygulama ve Reklam Ayarları

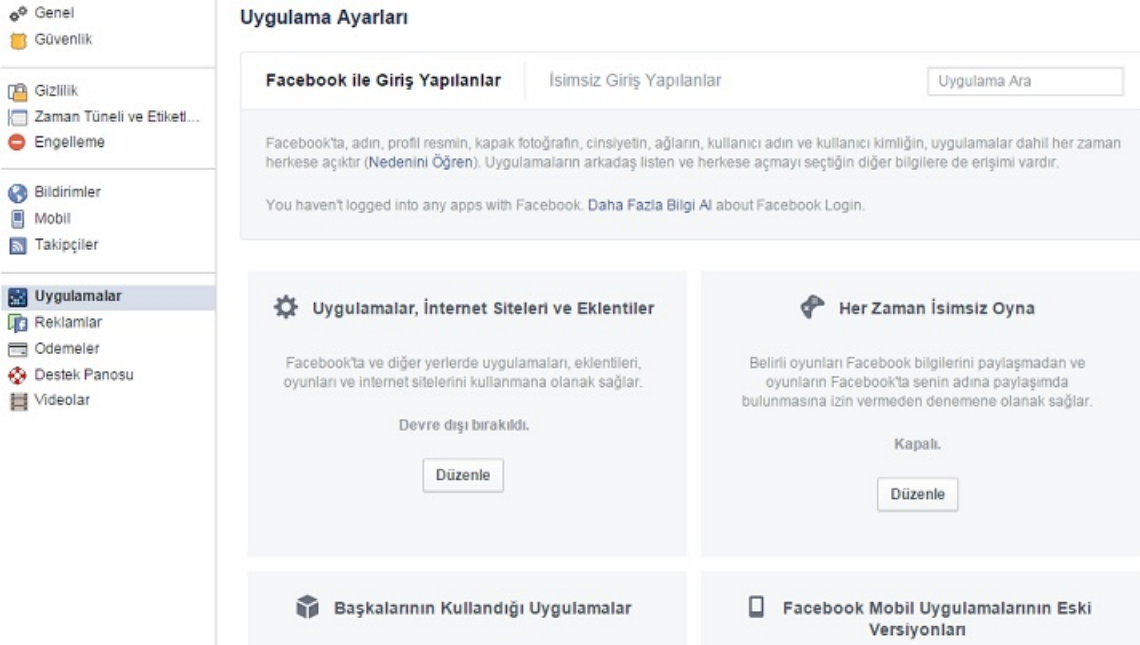
Bu sayfadaki kısımların listesi:

- [4.1 Uygulamalar](#)
- [4.2 Reklamlar](#)

## 4.1 Uygulamalar

**Facebook** kullanıcılarının çoğu *uygulamaları* çok sever ve onları aktif olarak kullanır – örneğin, oyunlar ve sosyal okuma alanları gibi iletişimi güçlendiren uygulamalar. Her uygulama **Facebook** hesabınız ile bağlantılıdır ve bu uygulamalar **Facebook** hesabınızdaki temel verilere (isminiz, cinsiyetiniz, halka açık fotoğraflarınız ve aığınız) ulaşabilir. Ek olarak, yeni bir uygulama indirdiğiniz zaman, uygulama, sizin ve arkadaşlarınızın bilgilerine ulaşp ulaşamayacağını sorabilir. Bu bilgilere, yaş, yaşanılan yer, eğitim ve arkadaş grubunuz gibi çeşitli veriler dahildir. Bu şekilde, uygulama, hangi ülkeden geldiğiniz ve şu anda nerede yaşadığınız gibi bilgilere erişip onları paylaşabilir. Bu bilgilerden bazıları sizin için hassas olabilir. Bu yüzden, güvenlik açısından, gerçekten kullanmak zorunda olmadığınız sürece, **Facebook** uygulamalarını kullanmamanızı öneririz.

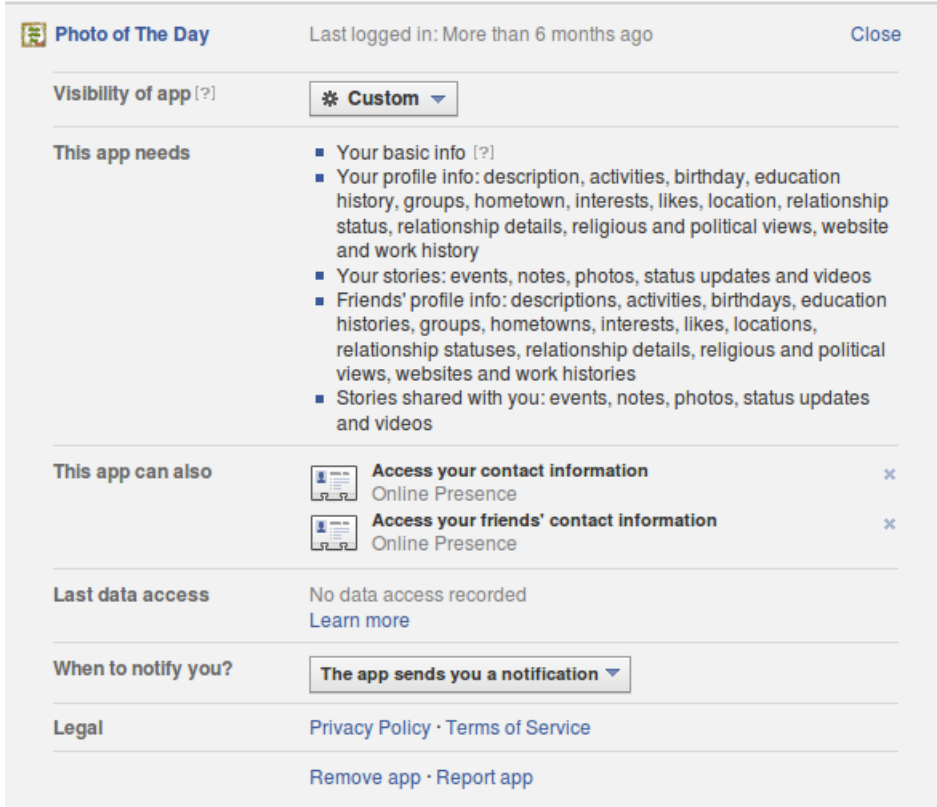
**1. Adım.** Soldaki menüden *Uygulamalar'ı* tıklayın.



Şekil 1: Uygulamalar menüsü

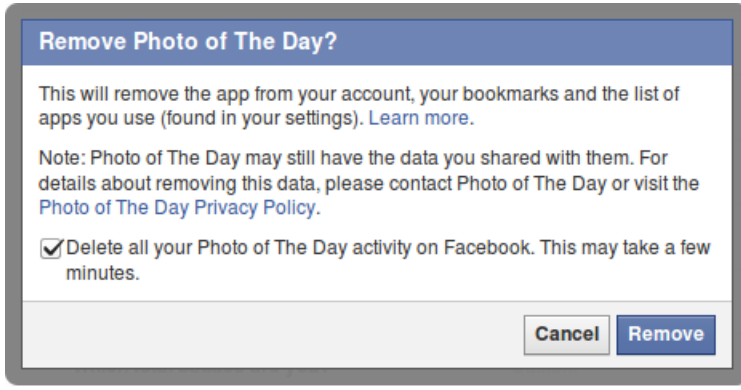
**2. Adım. Kullandığınız uygulamalar.** Buradan, Uygulamaları kullanmanıza olanak veren 'Facebook Platformu'nu etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu platform, örneğin, başka sitelere **Facebook** hesabınızı kullanarak kayıt olmanızı sağlar. Bu, bir yandan, kayıt formunu doldurmak ve tüm istenilenleri sağlamak ile vakit kaybetmenizi engellemek için iyi bir yöntem olabilir, özellikle de bu siteyi düzenli olarak kullanmayı düşünmüyorsanız (örneğin, haberlere yorum yazıyor veya bir imza kampanyasına katılıyorsanız). Fakat, diğer yandan, bu yöntemle, yorumunuz **Facebook** hesabınız ile bağlantılandırılır, kaydedilir ve paylaşımaya açık hale gelir. Yapacağınız şeyler için uygulamaları kullanmanız elzem değilse, güvenliğinizi korumak için **Platformu Devre Dışı Bırak'ı tıklamanızı** öneririz. Bu seçeneği etkin bırakmaya karar vererseniz, daha önceden kurulmuş olan uygulamalar listesini dikkatle incelemenizi tavsiye ederiz. Bunlara gerçekten de ihtiyacınız var mı?

**3. Adım.** Uygulamaların üzerine **tıklayarak** herbirinin hangi bilgilere erişimi olduğunu öğrenebilirsiniz.



Şekil 2: Uygulama detayları

**4. Adım.** Bir uygulamayı devre dışı bırakmak için, uygulamalar listesinin yanındaki 'x'e **tıklayın** ve açılan uyarı penceresinden **Kaldır'ı tıklayın**.



Şekil 3: Uygulama kaldır

**5. Adım. Başkalarının kullandığı uygulamalar.** Facebook arkadaşlarımızdan bazılarının kendi kullandığı uygulamalara bizim bilgilerimizi sağladığını da göz önünde bulundurmamız. *Başkalarının kullandığı uygulamalar'ı* tıklayarak arkadaşlarınızın uygulamaları ile paylaşmak istemediğiniz bilgi kategorileri kutularındaki işaretleri **kaldırabilirsiniz**.

**Başkalarının kullandığı uygulamalar** ×

Bilgilerini görebilen Facebook kullanıcıları, bu bilgileri kullandıkları uygulamalara taşıyabilir. Böylece kullandıkları uygulama daha kapsamlı ve sosyal hale gelir. İnsanların kullandıkları uygulamalara, oyunlara ve internet sitelerine taşıyabilecekleri bilgilerinin kategorilerini kontrol etmek için aşağıdaki ayarları kullan.

|                                                     |                                                                       |
|-----------------------------------------------------|-----------------------------------------------------------------------|
| <input type="checkbox"/> Biyografi                  | <input checked="" type="checkbox"/> Videolarım                        |
| <input type="checkbox"/> Doğum Tarihi               | <input type="checkbox"/> Bağlantılarım                                |
| <input type="checkbox"/> Aile ve ilişkiler          | <input type="checkbox"/> Notlarım                                     |
| <input type="checkbox"/> İlgilendikleri             | <input type="checkbox"/> Memleket                                     |
| <input type="checkbox"/> Dini inanç ve siyasi görüş | <input type="checkbox"/> Yaşadığın şehir                              |
| <input type="checkbox"/> İnternet sitem             | <input type="checkbox"/> Eğitim ve iş                                 |
| <input type="checkbox"/> Çevrimiçi olup olmadığım   | <input type="checkbox"/> Hobilerim, ilgi alanlarım, beğendiğim şeyler |
| <input type="checkbox"/> Durum güncellemelerim      | <input type="checkbox"/> Uygulama hareketlerim                        |
| <input type="checkbox"/> Fotoğraflarım              |                                                                       |

Uygulamaların ve internet sitelerinin diğer bilgi kategorilerine (arkadaş listen, cinsiyetin veya herkese açık yaptığın bilgilerin gibi) erişmesini istemiyorsan, tüm Platform uygulamalarını kapatabilirsin. Ancak bunu yaptığın takdirde, oyunları ve uygulamaları kullanamayacağını lütfen aklında bulundur.

Şekil 4: Başkalarının kullandığı uygulamalar

**6. Adım. Anında kişiselleştirme.** Facebook'un *Anında Kişiselleştirme* özelliği belli websitelerinin, onları ziyaret ettiğiniz zaman kamusal profil bilgilerinize erişmesini sağlar. Bu siteler web içeriklerini sizin istek ve ihtiyaçlarınıza adapte eder ve böylece kişiselleştirilmiş bir deneyim sunar. Daha güvenli olmak için, bulunduğunuz bölgede bu servis erişilebilir ise, onu **devre dışı bırakmanızı** öneririz.

**7. Adım. Anında Kişiselleştirme** sekmesinin altındaki **ıi tıklayın**. *Anında Kişiselleştirme'nin* ne olduğunu açıklamak için çıkan ekranda **ıi** tıklayın ve bir sonraki sayfanın alt kısmında *Partner websitelerinde anında kişiselleştirmeyi etkinleştir* kutusunun **işareti olmadığından** emin olun.

## 4.2 Reklamlar

Reklamlar, sosyal ağ şirketlerinin temel gelir kaynağı olduğu için çok önemlidir. Facebook gibi sosyal ağ sitelerinde mutlaka reklamlar yer alır, fakat onları bilgi güvenliği ve gizlilik için daha uygun olacak şekilde daha az kişisel hale getirmek mümkündür.

### 1. Adım. Soldaki kolondan *Reklamlar'ı* seçin

Facebook, isminizi ve fotoğrafınızı şimdilik reklamlarda kullanılmayacağına dair söz verse de, gelecekte bunun mümkün olabileceğine dair açık kapı bırakıyor. Gelecekte reklamlar ile ilgili politikaların değişme ihtimaline karşı bilgilerinizin

güvenliğini korumak için çeşitli ayarlar yapmanızı öneririz:

**2. Adım. Üçüncü Şahıs Siteleri'in yanında Düzenle'yi tıklayın.**

**3. Adım. Hiç Kimse'yi seçin ve Değişiklikleri Kaydet'i seçin.**

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Üçüncü Şahıs Siteleri</b> | <p>Facebook üçüncü şahıslara ait uygulamalara veya reklam ağlarına adını veya resmini reklamlarında kullanma hakkı vermez. Buna ilerde izin verirse, bilgilerinin nasıl kullanılacağını senin seçtiğin ayar belirleyecektir.</p> <p>Üçüncü şahıs sitelerinde, Facebook sosyal eklentileri üzerinden, reklamlardakiler dahil, sosyal bağlam görebilirsin. Sosyal eklentiler üçüncü şahıs sitesinde sosyal bir deneyim yaşamayı sağlasa da, Facebook bilgilerini sosyal eklentileri barındıran üçüncü şahıs sitelerle paylaşmaz. <b>Sosyal eklentiler</b> hakkında daha fazla bilgi al.</p> <p><b>Buna ilerde izin verirse, bilgilerimi şu kişilere gösterin:</b></p> <div><div>Hiç kimse</div></div> <div><div>Değişiklikleri Kaydet</div><div>İptal</div></div> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Şekil 6: Üçüncü Şahıs Siteleri Devre Dışı Bırakmak

**4. Adım. Sosyal Reklamlar. Burada \*\*Facebook**, kullanıcıları 'beğendikleri' sayfalardaki ürünlerin temsilcisi olmaya teşvik eder. Bu, sizin bir sayfanın veya bir ürünün reklamını arkadaşlarınıza yapmak için kullanılabileceğiniz anlamına gelir. Bu durumdan hoşnut değilseniz, bu seçeneği devre dışı bırakmanızı tavsiye ederiz.

**5. Adım. Reklamlar ve Arkadaşlar'ın altındaki Düzenle'yi tıklayın ve aşağı açılır menüden Kimse'yi seçin.**

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reklamlar ve Arkadaşlar</b> | <p>Herkes arkadaşlarının neleri sevdiğini bilmek ister. Bundan dolayı reklamları arkadaşlarıyla eşleştirerek arkadaşlarının paylaştığı ve beğendiği şeylere göre ilgini çekebilecek ürün ve hizmetleri kolayca bulmanı sağlıyoruz. <b>Sosyal reklamlar</b> hakkında daha fazla bilgi al.</p> <p>Sosyal reklamlarla ilgili bazı bilgiler:</p> <ul style="list-style-type: none"><li>■ Sosyal reklamlar, reklamverenin mesajını senin yapmış olduğun eylemlerle (bir Sayfa'yı beğenmek gibi) birlikte gösterir</li><li>■ Sosyal reklamlar senin gizlilik ayarlarına tabidir</li><li>■ Bilgilerini reklamverenlere satmayız</li><li>■ Bir reklamla birlikte gösterilen eylemlerini sadece onayladığın arkadaşların görebilir</li><li>■ Bir fotoğraf kullanılırsa, bu senin profil fotoğrafındır; fotoğraf albümlerinden alınmış herhangi bir fotoğraf değildir</li></ul> <p><b>Facebook Reklamlarına bir örnek:</b></p> <p>Bu ayar sadece sosyal eylemler hakkında haberleri eşleştirdiğimiz reklamlar için geçerlidir. Bu nedenle, bu ayardan bağımsız olarak, Sponsorlu Haberler veya Facebook'tan mesajlar gibi diğer bağlamlarda sosyal eylemleri görmeye devam edebilirsiniz. Sosyal reklamların, Sponsorlu Haberler'in ve Facebook'tan mesajların nasıl çalıştığı hakkında daha fazla bilgiyi Yardım Merkezi'nden alabilirsiniz.</p> <p><b>Reklamlarda sosyal eylemlerimi kimler görebilir:</b></p> <div><div>Hiç kimse</div></div> <div><div>Değişiklikleri Kaydet</div><div>İptal</div></div> |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Şekil 7: Sosyal Reklamları Devre Dışı Bırak

**6. Adım. Web sitesi ve telefon uygulamaları uyarlanmış kitleler. Facebook**, otomatik olarak, sizin zevk ve ilgi alanlarınızla uyumlu reklamları seçip göstermeye çalışır. Bu durumdan kurtulmak için, bu paragraftaki çıkış bağlantısına **tıklayın**.

Reklamların size ulaştığı yollardan biri, bir işletme veya kuruluşun Facebook'tan, reklamlarını Facebook dışındaki internet sitelerini veya uygulamalarını kullanan kişilere göstermesini istemesidir. Örneğin, bir şirketin ziyaret ettiğiniz internet sitesi ziyaretçilerini kaydetmek için çerezleri kullanıyor olabilir. Şirket daha sonra Facebook'tan reklamlarını bu ziyaretçi listesine göstermesini ister ve bu reklamları hem Facebook'ta hem de Facebook dışında görebilirsiniz. Bu, bir tür ilgi alanı tabanlı reklamdır.

Facebook'un veya diğer katılımcı şirketlerin, size reklam gösterme amacıyla Facebook dışındaki internet siteleri, cihazlar veya uygulamalardaki hareketlerinize dayalı olarak bilgi toplamasını veya kullanmasını istemiyorsanız, bunu ABD'de [Digital Advertising Alliance](#) üzerinden, Kanada'da [Digital Advertising Alliance of Canada](#) üzerinden veya Avrupa'da [European Digital Advertising Alliance](#) üzerinden durdurabilirsiniz. Bunu ayrıca mobil cihazınızın ayarlarını kullanarak da durdurabilirsiniz.

Durdurma işlemi yalnızca bir kez yapmanız gerekir. Facebook ilgi alanı tabanlı reklamlarını bir telefon veya bilgisayarda durdurursanız, bu seçiminizi Facebook'u kullandığınız her yere uygularız.

#### Şekil 8: 'Çıkış'ı seçin'

Bu şekilde, *Web sitesi ve Telefon uygulamalarınızdan uyarlanmış kitleler* sayfasını açabilirsiniz. Burada, Facebook reklam politikaları konusunda daha çok bilgi verir. Sayfanın ortasında, seçtikten sonra **onaylamanızı** gerektiren **çıkış** düğmesi vardır.

#### How can I stop seeing these ads?

If you don't want Facebook to show you ads based on your activity on an advertiser's websites or apps, opt-out below:

Opt out

Onaylama isteğinden sonra, şunu göreceksiniz:

✓ You have successfully opted out.

Opt in

**Aklınızda bulundurun:** Bu ayarlarda yapılan değişiklikler **Facebook'ta** kaydedilmek yerine tarayıcınızda saklanır. Bu yüzden, ne yazık ki, **Facebook'a** bağlanırken kullanacağınız her tarayıcı, uygulama ve araçta aynı işlemi **yeniden** yapmanız gerekir.

## Twitter Güvenlik Rehberi



**Twitter**, insanların 140 karakterlik *statü güncellemeleri* ile bilgi paylaştıkları bir sosyal ağıdır. Bu güncellemeler en başta 'şu anda ne yapmaktasınız?' sorusuna cevap vermekteydi, fakat daha sonra çok çeşitli bilgi türlerini yaymak için bir araca dönüştü. **Facebook'un** aksine **Twitter'da**, sadece tanıdığınız değil, ilginizi çeken herkesi 'takip edebilirsiniz'.

#### Ana Sayfa

- [www.twitter.com](http://www.twitter.com) [270]

#### Bilgisayar Gereksinimleri

- İnternet bağlantısı
- Güvenlik eklentileri olan **Firefox web tarayıcısı** [86] **Tor Tarayıcı** [192]

#### Bu bölümün son güncellenme tarihi

- Eylül 2014

#### Gerekli Okuma

- Nasıl Yapmalı Kitapçığı'nın **9. Bölüm'ü, Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz?** <sup>[256]</sup>
- **Twitter'in Kullanım Koşulları** <sup>[271]</sup> ve **Gizlilik Politikası** <sup>[272]</sup>

#### Buradan sağlayacağınız faydalar:

- **Twitter** kullanırken kamuya açık hale getirdiğiniz kişisel bilgilerin miktarını **azaltabilmek**.
- **Twitter'daki** statü güncelleme, fotoğraf ve diğer verilerinize kimin ve ne zaman ulaşabileceğini **kontrol etme** becerisi.
- Üçüncü taraflara açık olan bilgilerinizin miktarını **azaltabilmek**.

### 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

**Twitter**, kullanım şartlarında: 'Bu belge, Tweetlerinizi herkese açık hale getirmemiz için ve başkalarının da bunu yapabilmesi için bize yetki verdiğinizi gösterir. Fakat, size ait olan sizindir- ürettiğiniz içerik tümüyle size aittir.' yazar. Bununla birlikte, **Twitter**, talep edildiği takdirde, bilgilerinizi hükümetlere verme hakkını saklı tutar.

**Twitter'in** bir web sitesi olmasına rağmen, birçok insan **Twitter'ı**, **Twitter** istemcileri olarak bilinen masaüstü ve akıllı telefon uygulamaları üzerinden kullanır. Bir **Twitter** istemcisi kullanıyorsanız, onun siteye, şifrelenmiş bir bağlantı üzerinden güvenli bir şekilde bağlandığından emin olun. Bu konuyla ilgili olarak, **Bölüm 7: İnternet iletişiminizin gizliliği nasıl korunur?'un** <sup>[51]</sup> içindeki **E-postanızı güvenli kılmak'a** <sup>[273]</sup> bakın.

Ayrıca, **Facebook'a** benzer bir şekilde, birçok insan **Twitter'ı** statü güncelleme, fotoğraf, konum, bağlantı ve benzerlerini paylaşmak için başka web siteleri ve uygulamalar ile birlikte kullanır. Bu uygulamaları kullanmak olası birçok güvenlik zafafını beraberinde getirir, bu bakımdan bu uygulamaların gizlilik ayarlarını olabildiğince güvenli tutmak çok önemlidir.

Twitter, başta ABD olmak üzere, birçok hükümet tarafından aktif olarak denetlenir. Ek olarak, Twitter'ın Kullanım Şartları, devlet soruşturmaları gibi yasal talepler doğrultusunda bilgilerinizi paylaşabileceklerini belirtir. Daha fazla bilgi için Twitter'ın **Şeffaflık Raporu'na** <sup>[274]</sup> bakın.

## Twitter'da Temel Hesap Ayarları Nasıl Değiştirilir?

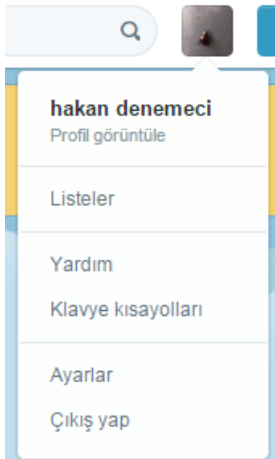
Bu sayfadaki kısımların listesi

- [2.1 Twitter Temel Hesap Ayarları](#)
- [2.2 Güvenlik ve Gizlilik Ayarları](#)
- [2.3 Parola Ayarları](#)
- [2.4 Mobil Ayarları](#)

### 2.1 Twitter Temel Hesap Ayarları

**Twitter** Temel Hesap Ayarları, insanların profilinize nasıl ulaşacağı, hangi bilgileri paylaşacağınız ve web tarayıcısı bazı **Twitter** versiyonunu kullanırken (herhangi bir istemci, akıllı telefon uygulaması ya da GSM telefonu yerine) hesabınızın gerektirdiği güvenlik seviyesinin ne olacağı konularını kontrol etmenize yarar.

**1. Adım.** Hesap ayarlarınıza ulaşmak için **Mozilla Firefox** <sup>[86]</sup> tarayıcısını kullanarak **hesabınıza giriş yapın** ve seçenekler menüsünü açmak için ekranın sağ üst köşesindeki ufak profil resminizi tıklayın.



Şekil 1: Seçenekler menüsü

**2. Adım.** Aşağı açılır menüden **Ayarlar'ı seçin**. Bu ayarlar sayfasını açacaktır. **3. Adım.** Ayarlar sayfasında, sol tarafta farklı ayar kategorilerine tıklayabileceğiniz bir sayfalar listesi vardır.

|                         |   |
|-------------------------|---|
| Hesap                   | > |
| Güvenlik ve gizlilik    | > |
| Şifre                   | > |
| Kartlar ve sevkیات      | > |
| Sipariş geçmişı         | > |
| Mobil                   | > |
| E-posta bildirimleri    | > |
| İnternet bildirimleri   | > |
| Sessize alınan hesaplar | > |
| Engellenmiş hesaplar    | > |
| Tasarım                 | > |
| Uygulamalar             | > |
| Bileşenler              | > |

Şekil 2: Ayarlar kategorileri

İlk kategori temel hesap ayarlarıdır

**4. Adım.** Hesap Ayarları listesinin üst kısmında, kullanıcı adı ve e-posta ayarlarını bulacaksınız. **Kullanıcı adı** olarak kendi adınızı mı yoksa bir rumuz mu kullanmak istediğinizi dikkatlice düşünün ve profilinize hangi e-posta adresini bağlayacağınıza karar verin. **Tor Tarayıcı** <sup>[192]</sup> kullanarak yeni bir **e-posta adresi almak** <sup>[172]</sup> iyi bir fikir olabilir, bu sayede **Twitter'a** sadece **Tor** kullanarak bağlanır ve kimliğinizi koruyabilirsiniz.

Kullanıcı Adı

HakanDenemeci

<https://twitter.com/HakanDenemeci>

Doğrulamak için e-postanı ([hakan.denemeci@riseup.net](mailto:hakan.denemeci@riseup.net)) kontrol et.

[Doğrulamayı yeniden gönder](#)

E-posta

[hakan.denemeci@riseup.net](mailto:hakan.denemeci@riseup.net)

E-posta herkes tarafından görülemeyecek. [Daha fazla bilgi al.](#)

Dil

Türkçe

Twitter çevirilerine yardım etmek ister misin? [Çeviri Merkezi'ne bir göz at.](#)

Zaman dilimi

(GMT+01:00) Belgrade

Şekil 2: Kullanıcı adı ve e-posta ayarları

## 2.2 Güvenlik ve Gizlilik Ayarları

**5. Adım.** Güvenlik ve gizlilik ayarları sayfasına ulaşmak için, sol taraftaki yan sekmede *Güvenlik ve gizlilik'e* **tıklayın**.

**6. Adım. Giriş Soruşturmaları.** Burada, **Twitter** hesabınıza erişildiği her anda cep telefonunuza veya akıllı telefonunuza bir mesaj gönderme seçeneğini sunar. **Twitter'ı** akıllı telefonunuzda da kullanıyorsanız bunu yapmanızı öneririz. Bu durumda, Giriş onaylamalarını *Twitter uygulamasına gönder'i* **seçin**.

**Aklınızda tutun** ki, bu seçeneği kullanmak, hesabınıza yapılan izinsiz bir girişten haberiniz olmasını sağlasa da, cep telefonunuzu Twitter hesabınız ile bağlantılandırmak sizi daha kolay bulunabilir hale getirecektir ve **Twitter'ı** anonim bir şekilde veya bir rumuzla kullanmak istiyorsanız tavsiye edilmez.

**7. Adım. Fotoğraf etiketleme.** Buradan **Twitter**, kimlerin yüklediği fotoğraflarda sizi etiketleyebileceğini kontrol etmenizi sağlar. Fotoğraflardaki etiketlemeyi *onaylama* veya *onaylamama* seçeneği olmadığı için, *Kimseinin beni fotoğraflarda etiketlemesine izin verme* seçeneğini seçin. Bu, özellikle eylemlerde fotoğrafınız çekildiği zaman, bunların daha sonra delil olarak kullanılmasını engeller.

- Fotoğraf etiketleme
- ☐ Başkalarının beni fotoğraflarda etiketlemesine izin ver.
  - ☐ Sadece takip ettiğim kişilerin beni fotoğraflarda etiketlemesine izin ver.
  - ☒ Kimsenin beni fotoğraflarda etiketlemesine izin verme.

Şekil 3: Etiketleme seçenekleri

**8. Adım. Tweet gizliliği.** Buradan **Twitter** tweetlerinizi, genel olarak herkesin mi yoksa sizi takip etmesine karar verdiğiniz kişilerin mi görebileceğini *kontrol etmenizi* sağlar. *Tweetlerimi koru* seçeneğini seçerseniz bile, tweetleriniz **Twitter'ın** erişimine açık olacaktır ve üçüncü taraflar ile paylaşılabılır bir şekilde kaydedilecektir.

**9. Adım. Tweet konumu.** Burada **Twitter**, tweetlerinize konum ekleme seçeneğini verir. Bu seçenek verili olarak devre dışı bırakılmıştır. Güvenli kalmanız için konumunuzu paylaşmanız gerekiyorsa bu seçenek faydalı olabilir. Fakat, genel olarak, bu özelliği **devre dışı bırakmanızı** öneririz çünkü konum bilgileriniz sizin aleyhinize kullanılabilir.

**10. Adım. Tanınabilirlik.** Burada **Twitter**, e-posta adresinize sahip olan insanların **Twitter** hesabınıza erişebilme seçeneğini sunar. Twitter hesabınız için daha fazla gizlilik istiyorsanız, bu seçeneği **devre dışı bırakmanızı** tavsiye ederiz.

- Keşfedilebilirlik
- ☐ Başkalarının beni e-posta adresimden bulmalarına izin ver

Şekil 4: Tanınabilirlik seçenekleri

**11. Adım. Kişiselleştirme ve tanıtım.** Burada **Twitter**, **Twitter** aktivitelerinizin denetlenmesi, gördüğünüz reklamların sizin aktivitelerinize göre şekillenmesi ve verilerinizin gerektiği zaman üçüncü taraflarla paylaşılabilmesi konuları ile ilgili seçenekler sunar. Daha fazla gizlilik için bütün bu kutulardaki **işaretleri kaldırmanızı** öneririz.

## 2.3 Parola ayarları

**12. Adım. Twitter** bu bölümde parolanızı değiştirmenize izin verir. Güçlü ve akılda kalıcı bir parola seçmenizi ve onu düzenli olarak güncellenenizi öneririz. Daha fazla bilgi için **Güvenli şifreler nasıl oluşturulur ve muhafaza edilir?** <sup>[157]</sup> bölümüne bakabilirsiniz.

### Şifre

Şifreni değiştir veya şimdikini kurtar.

Cep telefonunu gelişmiş güvenlik için Twitter hesabınla ilişkilendir.  
Daha fazla bilgi al.

Mevcut şifre

.....

Şifreni mi unuttun?

Yeni şifre

.....|

Çok Güçlü

Şifreyi doğrula

.....

Değişiklikleri kaydet

Şekil 5: Parola seçenekleri

**Twitter**, 'genişletilmiş güvenlik' için cep telefonunuzu Twitter hesabınız ile bağlantılandırmanız seçeneğini de verir. Yukarıda da belirttiğimiz gibi, bu bazı durumlarda faydalı olsa da, **Twitter** kullanırken kimliğinizi gizlemek istiyorsanız tavsiye edilmez.

**13. Adım.** Parolanızı güncelledikten sonra, *Değişiklikleri Kaydet'i* **tıklayın**.

## 2.4 Mobil Ayarları

**14. Adım.** Sol taraftaki menüden Mobil'i **tıklayarak** **Twitter** mobil ayarlarını **açabilirsiniz**.

Burada, **Twitter**, akıllı telefon uygulamasını indirmenize ve cep telefonunuzdan direk olarak tweet atabilmenizi sağlayan *Twitter mesaj yazma* seçeneğini etkinleştirmenizi teşvik eder. Yukarıda da belirttiğimiz gibi, **Twitter** hesabınız ile telefon

numaranızı bağlantılandırırsanız, tweet atarken belli bir gizlilik ve anonimlik istiyorsanız tavsiye edilmez. Ayrıca, GSM ağları üzerinden atılan **yazılı mesajlar** şifrelenmemiştir ve okunması ve kimin yazdığının teşhis edilmesi oldukça kolaydır. Daha fazla bilgi için, **Cep telefonları nasıl olabildiğince güvenli kullanılır?** <sup>[275]</sup> bölümüne bakabilirsiniz.

# Twitter İstemcileri ve Uygulamaları

Bu sayfadaki kısımların listesi:

- **3.0 Twitter İstemcileri ve Uygulamaları Esasları**
- **3.1 Instagram**
- **3.2 TwitPic**
- **3.3 Akıllı Telefon Uygulamaları**

## 3.0 Twitter İstemcileri ve Uygulamaları Esasları

**Twitter**, kullanıcılarının, örneğin **Instagram** ve **TwitPic** gibi websiteleri üzerinden yüklenmiş fotoğrafları paylaşmak için, hesapları ile etkileşime geçecek birçok başka sosyal ağ ve fotoğraf paylaşma sitesi kullanmasına izin verir. Fakat, **9. Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz** <sup>[256]</sup> bölümünde de belirttiğimiz gibi, farklı sosyal ağ sitelerindeki profillerinizi bir araya getirirken dikkatli olmalısınız. Kullandığınız diğer sitelerin kendi kullanım şartları, gizlilik politikaları ve güvenlik ayarları vardır ve bunların Twitter'inkinden farklı olabilir. Bu yüzden, **Twitter** hesabınız göreceli olarak güvenli olsa bile, profilleriniz diğer uygulama web sitelerinde teşhir edilebilir ve bu siteler için de aynı kullanıcı adı ve e-posta adresini kullanıyorsanız bu şekilde tespit edilebilirsiniz. Bu tür web siteleri ve uygulamaların sayısı oldukça fazladır. Bu kılavuzda bunlardan sadece birkaçına değiniyoruz. O yüzden, **Twitter** hesabınız ile birlikte kullandığınız diğer tüm siteler için araştırma yapmanızı ve güvenlik ayarlarınızı güncelleme tavsiye ederiz. Onları yeterince güvenli bulmuyorsanız, profilinizi silin ve **Twitter** hesabınıza erişimlerini engelleyin.

Herhangi bir uygulamanın **Twitter** profilinize erişimini engellemek istiyorsanız:

**1. Adım.** Hesabınızdaki **Ayarlar**'a gidin ve sol taraftaki sekmedeki **Uygulamalar**'ı **tıklayın**.

|                         |   |
|-------------------------|---|
| Hesap                   | > |
| Güvenlik ve gizlilik    | > |
| Şifre                   | > |
| Kartlar ve sevkıyat     | > |
| Sipariş geçmişi         | > |
| Mobil                   | > |
| E-posta bildirimleri    | > |
| İnternet bildirimleri   | > |
| Sessize alınan hesaplar | > |
| Engellenmiş hesaplar    | > |
| Tasarım                 | > |
| <b>Uygulamalar</b>      | > |
| Bileşenler              | > |

Şekil 1; Ayarlar menüsü

**2. Adım.** **Twitter** hesabınıza bağlanan uygulamalar listesini açtıktan sonra, hesabınıza erişmesini engellemek istediğiniz uygulamayı **seçin** ve **Erişimi kaldır** 'i **tıklayın**.

| Uygulamalar                                                                                                                                                                                                                                                                                             |                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Twitter hesabına erişimi olan uygulamalar. <a href="#">Daha fazla bilgi al.</a>                                                                                                                                                                                                                         |                                   |
|  <b>Facebook Bağlantısı</b><br>Tweetlerini Facebook profiline veya sayfana gönder.<br>Sorun mu yaşıyorsun? <a href="#">Daha fazla bilgi al.</a>                                                                        | <a href="#">Facebook'a bağlan</a> |
|  <b>TweetDeck</b> TweetDeck tarafından<br>TweetDeck is an app that brings more flexibility and insight to power users.<br>İzinler: okuma, yazma ve direkt mesaj<br>Onaylandı: 25 Mart 2015 Çarşamba 01:35:35           | <a href="#">Erişimi kaldır</a>    |
|  <b>Twitpic</b> Twitpic Inc tarafından<br>Share photos on Twitter with Twitpic<br>İzinler: okuma ve yazma<br>Onaylandı: 25 Mart 2015 Çarşamba 01:32:37                                                                 | <a href="#">Erişimi kaldır</a>    |
|  <b>Hootsuite</b> Hootsuite tarafından<br>The social media dashboard which allows teams to broadcast, monitor and track results.<br>İzinler: okuma, yazma ve direkt mesaj<br>Onaylandı: 25 Mart 2015 Çarşamba 01:30:41 | <a href="#">Erişimi kaldır</a>    |

Şekil 2: Uygulamalar listesi örneği

### 3.1 Instagram

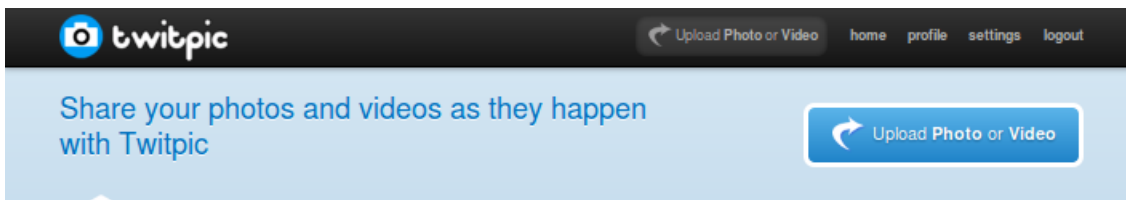
**Instagram**, **Facebook'a** <sup>[276]</sup> ait, popüler bir imaj-paylaşım akıllı telefon uygulamasıdır ve genellikle **Twitter** ile birlikte kullanılır. **Instagram**, öncelikli olarak bir cep telefonu uygulaması olduğu için, **Twitter** ile birlikte kullanıldığı zaman, hesabınızı cep telefonunuz ile bağlantılandırır ve bu da bulunduğunuz konum gibi birçok bilginin, **Facebook**, **Instagram**, ve **Twitter** ile, dolayısıyla, devlet dahil olmak üzere üçüncü taraflar ile paylaşılabilmesi anlamına gelir. Bu yüzden de, hassas bir bilgi akışında bulunuyorsanız, **Instagram'ı** aynı hesapla ve hatta aynı cihazda kullanmamanızı tavsiye ederiz.

### 3.2 TwitPic

Birçok **Twitter** kullanıcısı, **Twitter** üzerinden paylaştıkları fotoğrafları yüklemek ve saklamak için **TwitPic** web sitesini kullanır. Unutmayın ki **TwitPic**, **Twitter'a** ait olmayan ayrı bir şirkettir ve farklı Kullanım Şartları ve Gizlilik Politikası vardır. **TwitPic** kullanıcılarına profillerini ve fotoğraflarını saklama olanağı tanımaz. **TwitPic'e** yüklenen tüm fotoğraflar verili olarak halka açıktır ve bu değiştirilemez. **Twitter** ve **TwitPic** hesaplarınız için aynı kullanıcı adını kullanıyorsanız, istemediğiniz kişiler **TwitPic'e** yüklediğiniz tüm fotoğraflara kolayca erişebilir.

**TwitPic** diğer kullanıcıların kendi fotoğraflarında sizi etiketlemesine izin verir. Hassas bir fotoğrafta sizi etiketlemeleri halinde bu durum riskli olabilir, çünkü bu şekilde bu bilgiler halka açık hale gelecektir. Bu yüzden, diğer kullanıcıların fotoğraflarında sizi etiketlemesini engellemeyi tavsiye ederiz.

**1. Adım.** **TwitPic** hesabınıza **Firefox** tarayıcısını kullanarak giriş yapın ve ekranın sağ üst köşesindeki menüden *Ayarlar'ı* tıklayın.



Şekil 3: TwitPic ana sayfa menü çubuğu

**2. Adım.** **Gizlilik** seçeneğinin altında *Başkalarının benim fotoğraflarımı etiketlemesine izin ver* kutusundaki **işareti kaldırın** ve **Değişiklikleri Kaydet'i** tıklayın.

## Privacy

Show my updates in the public timeline ☐

Allow others to tag my photos ☐

Save Changes

Şekil 4: Etiketleme seçenekleri

TwitPic'ten hassas imajları silmek istiyorsanız:

**3. Adım.** Ekranın üst sağ köşesindeki menüden *Profil'i* **tıklayın**.

**4. Adım.** Silmek istediğiniz fotoğrafın yanındaki *Sil'i* **tıklayın**.

Photos and Videos by @shmooby1234

Timeline Gallery



about a minute ago via site 0

delete

1

Şekil 5: İmaj Seçenekleri

TwitPic hesabınızı silmek istiyorsanız:

**5. Adım.** Ekranın sağ üst köşesindeki menüden *Ayarlar'ı* **tıklayın**.

**6. Adım.** *Hesabı Sil'in* altındaki kutuya 'captcha' imajında görünen kelimeleri **yazın**.

## Delete Account

If you would like to delete your account, you may do so here. Enter the captcha first to continue.

happy. yasoul

Geben Sie die 2 Wörter ein:

happy yasoul

reCAPTCHA™ stop spam. read books.

Delete Account

Şekil 6: Profilinizi silmeden önce bu 'captcha' imajı görünecektir.

**7. Adım.** **Delete Account** 'ı tıklayın.

## 3.3 Akıllı Telefon Uygulamaları

iPhone, Android, Blackberrys ya da Windows Telefonları gibi akıllı telefonlar için, **Twitter** ile eş zamanlı kullanılabilecek bir dizi İstemci ve Uygulama mevcuttur. Akıllı telefonların birçok güvenlik zaafı olduğu unutulmamalıdır, bu yüzden de bu Uygulama ve İstemcileri akıllı telefonlarda kullanmak bilgisayarda kullanmaktan daha az güvenli olabilir. Örneğin, bunlar **Twitter'a** şifrelenmemiş bir bağlantı üzerinden bağlanarak tweetlerinizi ifşa edebilir. Akıllı telefon kullanırken oluşan riskleri

azaltmak için **Akıllı telefonlar nasıl olabildiğince güvenli kullanılır?** <sup>[277]</sup> bölümüne bakabilirsiniz.

# YouTube



**YouTube**, **Google'a** ait, kullanıcıların video yükleme ve paylaşmasını sağlayan bir servistir. İnsan hakları savunucuları arasında, diğer başka konularla birlikte insan hakları ihlalleri kanıtlarını paylaşmak için sıklıkla kullanılır hale gelmiştir.

## Ana sayfa

- <https://www.youtube.com/> <sup>[278]</sup>

## Bu bölümün son güncellenme tarihi

- Eylül 2014

## Bilgisayar Gereksinimleri

- İnternet bağlantısı
- [Güvenlik eklentileri ile Firefox web tarayıcısı](#) <sup>[86]</sup> ya da [Tor Tarayıcı](#) <sup>[192]</sup>

## Gerekli Okuma

- Kullanma Kılavuzu **9. Bölüm Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz** <sup>[279]</sup>
- **YouTube Kullanım Şartları** <sup>[280]</sup> Ve **Google Gizlilik Politikası** <sup>[281]</sup>

## Burada Sağlayacağınız Faydalar::

- Video malzemelerini YouTube üzerinden paylaşıırken kendinizin ve diğerlerinin gizliliğini nasıl koruyabileceğiniz konusunda ipuçları.

## 1.1 Başlamadan önce bu araçla ilgili bilmeniz gerekenler

**YouTube** videonuza milyonlarca kullanıcının erişmesi için oldukça faydalıdır. Fakat, **YouTube Google'un** malıdır, **Google** çalışanları videonuzu zararlı bulursa onu silebilir. **Google** kullanıcıların meta verilerini toplayıp, Amerika dahil olmak üzere çeşitli hükümetlerle paylaşabilir. Ayrıca, **Google** videolarınızla ilgili spesifik bilgileri (örneğin konum verileri) talep edilmesi halinde devlet aygıtları ile paylaşabilir. Bu da demektir ki filminizi güvenli tutmak için **YouTube** çok uygun bir yer değildir. **Google'in** aynı zamanda, sitenin sansürlenmesini engellemek için baskılara boyun eğerek **Youtube'dan** çeşitli içerikleri kaldırmış olduğu bilinmektedir. Eğer insanların videonuzu görmesini istiyorsanız, videonuzun bir kopyasını **YouTube'a** yerleştirebilirsiniz, fakat **Youtube'da** video saklama açısından güvenli olmadığı için oraya yüklediğiniz kopyanın elinizdeki tek kopya olmamasına dikkat edin.

**YouTube'a** koyduğunuz içerikler sizindir ama onları **YouTube'a** koyarak **Google'a** bu bilgileri paylaşabilmesi için ehliyet vermiş oluyorsunuz.

**YouTube'un** çeşitli ülkelerde erişime kapalı olduğu bilinmektedir, örneğin:

- Çin
- Burma
- İran
- Libya
- Suriye
- Özbekistan
- Tunus
- Türkmenistan
- Türkiye

Bugün ve geçmişte yaşanmış sansür ve diğer kesintiler ile ilgili daha fazla bilgi almak istiyorsanız **Şeffaflık Raporu'ndaki Google trafiği bölümüne** <sup>[282]</sup> bakabilirsiniz.

## YouTube ile ilgili tüyolar:

- Videosu çekilen kişinin izni olmadan hiçbir videoyu paylaşmayın. Kişi izin verse bile, paylaşmanın getireceği sonuçları dikkatlice tartın.
- **YouTube'a** ulaşmak için tarayıcınızın adres çubuğuna <https://www.youtube.com> yazın - bu şekilde, bilgisayarınız ve **YouTube** sunucuları arasındaki iletişim, **Güvenli Soket Katmanı** (SSL) bağlantısı ile şifrelenmiş olacaktır.

Bağlandığınız her seferde bunu tekrar etmemek için, **YouTube'a HTTPS Everywhere** <sup>[283]</sup> gibi eklentiler ile **Firefox** <sup>[86]</sup> kullanarak bağlanmanızı öneririz

- Daha fazla gizlilik için, sadece **Tor Tarayıcı** <sup>[193]</sup> kullanırken yaratılmış ve erişilen yeni ve anonimleştirilmiş bir Google hesabı yaratın. **YouTube'a** video yüklemek için bu hesabı kullanın, böylece konumunuz ve diğer verileriniz **Google'dan** ve İnternet Servis Sağlayıcınızdan gizli tutulabilir. Fakat, **YouTube'daki** videoları **Tor Tarayıcı** ile görüntülemek genellikle zordur. Videoları izlemek için, başka bir hesap yaratmak ve **Eklentili Firefox** <sup>[284]</sup> gibi bir tarayıcı kullanmak en iyisidir.
- Herhangi bir **Android** <sup>[285]</sup> cihazından hassas videolar yüklemek için **Guardian Project'in** <sup>[286]</sup>, **InformaCam** <sup>[287]</sup> uygulamasını kullanmayı düşünebilirsiniz. Bunlar, kullanıcılara videolarının meta verileri üzerinde daha fazla kontrol sahibi olmalarını sağlar ve **Orbot** <sup>[288]</sup> ile birlikte kullanıldığı zaman Tor ağı üzerinden yükleme yapmayı kolaylaştırır.
- İnsanların tanınmak istemeyebeileceği, örneğin protesto videolarında **YouTube'un** yüz-buğulama seçeneğini kullanın. **Buradan** <sup>[289]</sup> bu konu üstüne daha fazla bilgi edinebilirsiniz.
- **YouTube** üzerinden paylaştığınız tüm videoların bir kopyasını saklayın.
- Videolarınızı sadece seçtiğiniz kişilerle paylaşmak için *gizli* ayarını seçin.

## YouTube Alternatifleri

Videolarınızı **Google profiliniz** ile ilişkilendirmek istemiyorsanız, **Vimeo** <sup>[290]</sup> gibi çeşitli alternatifler mevcuttur. Vimeo'nun kullanıcıları **YouTube'dan** azdır. **YouTube** gibi, Vimeo da **SSL** üzerinden bağlantıya izin verir ve kullanıcılarına çeşitli gizlilik seçenekleri ve videolar için yaratıcı müşterek lisansların kontrolünü sunar. Farklı bölgelerde başka benzer siteler kullanılıyor olabilir, kendi araştırmanızla bunlara ulaşabilirsiniz. Birini kullanmaya başlamadan önce aşağıdaki noktaları göz önünde bulundurunuz:

1. Sadece giriş yaparken değil, sitenin tüm kullanımları için **SSL** üzerinden bağlantı sağlıyor mu? Şifreleme sertifikaları dahil olmak üzere şifreleme ile ilgili problemleri var mı?
2. Son Kullanıcı Lisans Anlaşmasını, Gizlilik Politikasını veya Data Kullanım Politikasını dikkatlice okuyun. İçeriğiniz ve kişisel verileriniz nasıl kullanılıyor? Kimlerle paylaşılıyor?
3. Kullanıcılar için hangi gizlilik seçenekleri sağlanmış? Videolarınızı seçtiğiniz kimselerle paylaşma imkanınız var mı, yoksa verili olarak halka açık hale mi geliyorlar?
4. Protesto görüntüleri gibi hassas imajlar yüklüyorsanız, site, yüz-buğulama gibi yöntemlerle filme çekmiş olduğunuz kimselerin güvenliğini sağlıyor mu?
5. Sunucuların coğrafi konumunu, hangi bölgesel hukuk kurallarına tabi olduklarını veya şirketin nerede kayıtlı olduğunu biliyor musunuz? Bu bilgilerin, e-posta aktiviteleriniz ve bilgilerinizin gizlilik ve güvenliği bakımından ne anlama geldiğini biliyor musunuz? Sitenin sahipleri, hükümetten bir talep geldiği takdirde bilgilerinizi paylaşacak mı?

## Flickr



Flickr, **Yahoo!'ya** ait popüler bir imaj barındırma ve paylaşma web sitesidir.

### Ana sayfa

- <https://secure.flickr.com/> <sup>[291]</sup>

### Bu bölümün son güncellenme tarihi

- Eylül 2014

### Bilgisayar Gereksinimleri

- İnternet bağlantısı
- [Güvenlik eklentileri ile Firefox web tarayıcısı](#) <sup>[86]</sup> ya da [Tor Tarayıcı](#) <sup>[192]</sup>

### Required Reading

- Nasıl Yapmalı Kitapçığı'nın **9. Bölüm'ü Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz** <sup>[279]</sup>
- [Flickr'ın Kullanım Koşulları](#) <sup>[292]</sup> ve [Gizlilik Politikası](#) <sup>[293]</sup>

### Buradan Sağlayacağınız Faydalar:

- Flickr kullanarak fotoğraflarınızı paylaşıırken kendi gizliliğinizi ve diğerlerinizin güvenliğini sağlamak için tüyolar.

## 1.1 Başlamadan önce bu cihazla ilgili bilmeniz gerekenler

**Flickr Yahoo!'**ya aittir ve **Google** ve **Facebook** da dahil olmak üzere diğer hesaplarla birlikte kullanılması kolaylaştırılmıştır. **Flickr'da** paylaştıklarınız size ait kalır ve bunlara farklı yaratıcı müşterek lisansları ve telif hakkı atfedebilirsiniz. İçerik paylaşarak **Yahoo!'**ya fotoğraflarınızı ve videolarınızı dağıtma ehliyeti verirsiniz. Farklı lisans atfetmeleri sebebiyle, **Flickr** kampanyalarda kullanılabilecek resimler bulmak için olduğu kadar ve meslektaş, arkadaş ve ağındaki insanlarla imaj paylaşmak için çok iyidir. Fakat, **Flickr** kullanıcı verilerinin çeşitli hükümetler tarafından toplanıp ve kontrol edildiği ihtimali de çok yüksektir.

Daha fazla bilgi için, Yahoo!'nın **Gizlilik Politikası'nı** <sup>[294]</sup> okuyun.

## Flickr gizlilik ayarlarının güncellenmesi

**1. Adım.** Flickr Gizlilik ve İzinler ayarlarına erişmek için, **Mozilla Firefox** tarayıcısı kullanarak **Flickr** hesabınıza **giriş yapın** ve ekranın sağ üst köşesinde ikona **basın** ve **Ayarlar'ı** seçin

**2. Adım.** Ana *ayarlar* sayfasından **Gizlilik ve İzinler'i** seçin.

### Your account

|                           |                                                                                                                                                                                                                                                                        |                        |                     |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---------------------|
| Personal Information      | Privacy & Permissions                                                                                                                                                                                                                                                  | Emails & Notifications | Sharing & Extending |
| Your Flickr account       | You are signed in to Flickr via your Yahoo ID ( <b>onois insecure</b> )<br>You have a Flickr account where you get a free terabyte of space for original photos and HD videos.                                                                                         |                        |                     |
| Your safety level         | Not set. For more info, click <a href="#">here</a> .                                                                                                                                                                                                                   |                        |                     |
| Your buddy icon           |  <a href="#">edit</a>                                                                                                                                                                 |                        |                     |
| Your screen name          | OnoRobot <a href="#">edit</a>                                                                                                                                                                                                                                          |                        |                     |
| Your profile              | <ul style="list-style-type: none"><li>Tell people a little (or a lot) about yourself (or, <a href="#">view your profile page</a>)</li><li>For your profile, <a href="#">edit who can see what</a> or <a href="#">if it's searchable</a></li></ul> <a href="#">edit</a> |                        |                     |
| Your Flickr web addresses | <a href="#">Create your own memorable Flickr web address!</a> It's an easy way to share your Flickr profile and your photostream with your friends                                                                                                                     |                        |                     |

Şekil 2: Flickr Gizlilik ve İzinler ayarları

**3. Adım.** Flickr verili olarak fotoğraflarınızı herkese açık hale getirir. Daha fazla gizlilik istiyorsanız, *Orijinal İmaj dosyalarınıza kimler erişebilir?* seçeneğinde **düzenle'yi** **tıklayın** ve **Sadece ben'i** **seçin** ve **Kaydet'i** **tıklayın**.

#### Who should be able to access your original image files and other sizes without deterrents?

- ☒ Only you  
☐ Your friends and family  
☐ People you follow  
☐ Any Flickr member  
☐ Anyone (Recommended)

**SAVE** **CANCEL**

Şekil 3: Orijinal İmaj dosyalarınıza kimler erişebilir?

**4. Adım.** Verili olarak, **Flickr**, içeriğinize erişimi olan insanların onları Facebook ve Twitter gibi sitelerde paylaşmasına izin verir. Bu da, hassas imajların kolayca yanlış ellere geçmesine neden olabilir. İmajların nasıl paylaşılacağına karar veren kişi olmak istiyorsanız, bu seçeneği devre dışı bırakmanızı öneririz. Bunu yapmak için, *Başkalarının sizin paylaşımlarınız paylaşmasına izin ver'in* yanındaki **düzenle'yi** **tıklayın** ve **Hayır, teşekkürler'i** **seçin**. Daha sonra, **Kaydet'i** **tıklayın**.

## Allow others to share your stuff

You can set a preference that determines whether sharing features (such as Facebook, Twitter, Tumblr and others) are shown for other people on your public content. These features will always show for you on your content.

☐ Yes please, that would be lovely

☒ No, thanks

SAVE

Or, cancel this and return [to your account page](#).

Şekil 4: Başkalarının sizin paylaşımlarınız paylaşmasına izin ver

**5. Adım.** Verili olarak, **Flickr** diğer kullanıcıların sizi fotoğraflarda etiketlemesine izin verir. Bu durum, örneğin bir protesto veya herhangi bir sivil itaatsizlik eylemi fotoğrafında etiketlenmeniz gibi tehlikeli bir sonuca yol açabilir. Bu yüzden, sizi fotoğraflarda sizden başka kimsenin etiketleyememesi için, *Sadece ben* seçeneğini seçmenizi **tavsiye ederiz**.

## Who can add you to a photo?

You can set a preference that determines whether or not other members can mark you as being in a photo.

- ☒ Only you
- ☐ Your friends and family
- ☐ Your family
- ☐ Your friends
- ☐ People you follow
- ☐ Any Flickr member (Recommended)

SAVE

Or, cancel this and return [to your account page](#).

Şekil 5: Başkalarının etiketlemesini devre dışı bırak

**6. Adım.** Verili olarak, **Flickr** sizin **EXIF** verilerinizi (fotoğrafların çekildiği kameranın modeli, fotoğrafın çekilme yeri ve zamanı gibi meta veriler) diğer kullanıcılarla paylaşır. Bu bilgiler hassas olabileceği için paylaşmamanızı tavsiye ederiz.

## Who can see your EXIF data?

Hide my EXIF data? ☒ Yes

SAVE CHANGES

Or, cancel and [return to your account page](#).

Şekil 6: EXIF veri seçenekleri

**7. Adım.** Verili olarak, **Flickr** fotoğraflarınızı ve kamusal profilinizi arama motorları üzerinden herkese açık hale getirir. Kimlerin bilgi ve fotoğraflarınıza ulaşabileceği konusunda daha fazla kontrol sahibi olmak istiyorsanız, herkese açık aramalara profil ve fotoğraflarınızı **kapatmanızı** tavsiye ederiz.

|                                             |                                        |
|---------------------------------------------|----------------------------------------|
| Hide your stuff from public searches<br>[?] | Yes, on flickr.com and 3rd-party sites |
| Hide your profile from public searches      | Yes                                    |

Şekil 7: Herkese açık arama seçenekleri

**8. Adım. Yeni yüklemeler:** **Flickr**'ın verili ayarları, yeni bir içerik yüklediğiniz zaman, olabildiğince çok bilginin paylaşılmasını ve mümkün olduğunca yüksek bir etkileşimi amaçlar. Daha fazla gizlilik içeren seçenekleri seçmenizi öneririz, örneğin:

- Yeni yüklediğiniz fotoğrafları diğerlerinin anında görmesini, paylaşmasını veya onlara yorum yapmasını engellemek
- Yeni yüklediğiniz fotoğrafların konuma bilgilerinin başkaları tarafından görülmesini engellemek
- Yeni yüklediğiniz fotoğrafları yalnızca belli kişilerin erişimine açmak

Bu ayarlar her yükleme için değiştirilebilir, örneğin EXIF verilerini delil olarak eklemek istediğiniz zaman bu ayarları değiştirebilirsiniz.

## Defaults for new uploads

|                                                               |                                                                                                                                                 |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Who will be able to see, comment on, add notes, or add people | <ul style="list-style-type: none"><li>• View: Only you</li><li>• Comment on: Only you</li><li>• Add notes, tags, and people: Only you</li></ul> |
| What license will your content have                           | All rights reserved ©                                                                                                                           |
| Who will be able to see your stuff on a map                   | Only you                                                                                                                                        |
| Import EXIF location data [?]                                 | No                                                                                                                                              |
| Auto-rotate your photos [?]                                   | Yes                                                                                                                                             |
| What Safety Level and Content Type will your photostream have | <ul style="list-style-type: none"><li>• Safety level: Restricted</li><li>• Content type: Photos</li></ul>                                       |

Şekil 8: Yeni yüklemeler için daha fazla gizlilik içeren seçenekler

## Flickr Alternatifleri:

Fotoğraflarınızı Yahoo, Google veya Facebook profilleriniz ile ilişkilendirmek istemiyorsanız, çeşitli alternatifler mevcuttur. Başka bölgelerde başka benzer siteler kullanılıyor olabilir, farklı seçenekler arıyorsanız bunları araştırabilirsiniz. Birini seçmeden önce aşağıdaki noktaları göz önünde bulundurmalısınız:

1. **SSL** üzerinden bağlantıyı sadece giriş aşamasında mı, yoksa sitenin tüm kullanımları için mi sağlıyor? Şifreleme sertifikaları benzeri şifreleme problemleri var mı?
2. Son Kullanıcı Lisans Anlaşması, Gizlilik Politikası ve Veri Kullanma Politikası'nı dikkatle okuyunuz. İçeriğiniz ve kişisel verileriniz nasıl kullanılıyor? Kimlerle paylaşılıyor?
3. Kullanıcılar için hangi gizlilik seçenekleri sağlanmış? Fotoğraflarınızı küçük bir grup insan ile güvenli bir şekilde paylaşabiliyor musunuz, yoksa verili olarak kamuya açık durumdalar mı?
4. Örneğin bir protesto fotoğrafı gibi hassas bir fotoğraf yüklediğiniz zaman, fotoğrafını çektiğiniz insanları yüz-buğulama gibi yöntemler kullanarak koruyor mu?
5. Sunucuların coğrafi konumunu, hangi yerel hukuk sistemlerine bağlı olduğunu ve şirketlerin nereye kayıtlı olduğunu biliyor musunuz? Bu bilgilerin sizin e-posta aktivite ve bilgilerinizin gizlilik ve güvenliği bakımından ne anlama geldiğinden haberdar mısınız? Sitenin sahibi olan kimseler, herhangi bir hükümetten istek geldiği takdirde bilgilerinizi paylaşır mı?

Source URL (retrieved on 16/06/2015 - 12:06): <https://info.securityinabox.org/tr/handsonguides>

### Bağlantılar:

- [1] <https://info.securityinabox.org/tr/handsonguides>
- [2] <http://www.keepass.info/download.html>
- [3] <http://www.keepass.info/>
- [4] <https://info.securityinabox.org/tr/chapter-3>
- [5] <http://www.keepassx.org/>
- [6] <http://passwordsafe.sourceforge.net/>
- [7] <http://agilewebsolutions.com/products/1Password>
- [8] <https://info.securityinabox.org/sbox/programs/KeePass-Setup.exe>
- [9] <http://keepass.info/translations.html>
- [10] [https://info.securityinabox.org/tr/keepass\\_passwords](https://info.securityinabox.org/tr/keepass_passwords)
- [11] [https://info.securityinabox.org/tr/keepass\\_portable](https://info.securityinabox.org/tr/keepass_portable)
- [12] <http://keepass.info/download.html>
- [13] [https://info.securityinabox.org/en/keepass\\_main](https://info.securityinabox.org/en/keepass_main)
- [14] <https://info.securityinabox.org/sbox/programs/KeePass.zip>
- [15] <https://info.securityinabox.org/tr/recuva>
- [16] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%20Setup%207.1a.exe>
- [17] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%20Setup%207.1a.exe.sig>
- [18] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Mac%20OS%20X.dmg>
- [19] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Mac%20OS%20X.dmg.sig>
- [20] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x86.tar.gz>
- [21] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x86.tar.gz.sig>
- [22] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x64.tar.gz>
- [23] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x64.tar.gz.sig>
- [24] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x86.tar.gz>
- [25] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x86.tar.gz.sig>
- [26] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x64.tar.gz>
- [27] <https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x64.tar.gz.sig>
- [28] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Source.zip>
- [29] <https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Source.zip.sig>
- [30] <https://info.securityinabox.org/sbox/programs/truecrypt/VersionHistory.txt>
- [31] <https://keys.mozilla.org/pks/lookup?op=get&search=0xE3BA73CAF0D6B1E0>

[32] <https://info.securityinabox.org/sbox/programs/truecrypt/F0D6B1E0.asc>  
[33] <https://www.torproject.org/docs/verifying-signatures.html.en>  
[34] <https://truecrypt.ch/downloads/>  
[35] [https://securityinabox.org/tr/truecrypt\\_portable](https://securityinabox.org/tr/truecrypt_portable)  
[36] <https://info.securityinabox.org/chapter-4>  
[37] <http://www.ubuntu.com/>  
[38] <http://www.saout.de/misc/dm-crypt/>  
[39] <http://code.google.com/p/cryptsetup/>  
[40] <http://sd4l.sourceforge.net/>  
[41] [https://diskcryptor.net/wiki/Main\\_Page](https://diskcryptor.net/wiki/Main_Page)  
[42] <http://www.axantum.com/AxCrypt/>  
[43] <http://windows.microsoft.com/en-us/windows7/products/features/bitlocker>  
[44] <https://info.securityinabox.org/sbox/programs/TrueCrypt-Setup.exe>  
[45] [http://securityinabox.org/tr/truecrypt\\_portable](http://securityinabox.org/tr/truecrypt_portable)  
[46] <http://andryou.com/truecrypt/docs/index.php>  
[47] <http://www.truecrypt.org/docs/>  
[48] [https://info.securityinabox.org/tr/truecrypt\\_hiddenvolumes](https://info.securityinabox.org/tr/truecrypt_hiddenvolumes)  
[49] <http://www.gpg4usb.org/download.html>  
[50] <http://www.gpg4usb.org/>  
[51] <https://info.securityinabox.org/tr/chapter-7>  
[52] <https://www.frontlinedefenders.org/esecman>  
[53] <https://info.securityinabox.org/sbox/programs/gpg4usb.zip>  
[54] <https://info.securityinabox.org/sbox/screen/gpg4usb-en-1/03.png>  
[55] [https://info.securityinabox.org/tr/thunderbird\\_main](https://info.securityinabox.org/tr/thunderbird_main)  
[56] <https://securityinabox.org/tr/node/2276#4.1>  
[57] <http://www.piriform.com/ccleaner/builds>  
[58] <http://www.ccleaner.com>  
[59] <https://info.securityinabox.org/tr/chapter-6>  
[60] <http://bleachbit.sourceforge.net/>  
[61] <https://info.securityinabox.org/tr/chapter-5>  
[62] <https://info.securityinabox.org/sbox/programs/ccsetup.exe>  
[63] [https://info.securityinabox.org/en/ccleaner\\_faq](https://info.securityinabox.org/en/ccleaner_faq)  
[64] <http://www.piriform.com/ccleaner/download/portable>  
[65] [https://info.securityinabox.org/tr/ccleaner\\_main](https://info.securityinabox.org/tr/ccleaner_main)  
[66] <https://info.securityinabox.org/sbox/programs/ccsetup.zip>  
[67] [https://info.securityinabox.org/tr/ccleaner\\_portable](https://info.securityinabox.org/tr/ccleaner_portable)  
[68] <https://riseup.net/>  
[69] <https://help.riseup.net/en/about-us>  
[70] [http://securityinabox.org/tr/thunderbird\\_main](http://securityinabox.org/tr/thunderbird_main)  
[71] <https://lists.riseup.net/>  
[72] <https://we.riseup.net/>  
[73] <https://pad.riseup.net/>  
[74] <https://help.riseup.net/en/vpn>  
[75] <https://info.securityinabox.org/tr/chapter-8>  
[76] <https://help.riseup.net/en/chat>  
[77] <https://info.securityinabox.org/tr/jitsi>  
[78] [https://info.securityinabox.org/tr/pidgin\\_main](https://info.securityinabox.org/tr/pidgin_main)  
[79] [https://info.securityinabox.org/tr/chapter\\_7\\_3](https://info.securityinabox.org/tr/chapter_7_3)  
[80] [https://info.securityinabox.org/tr/riseup\\_changingsettings#4.3](https://info.securityinabox.org/tr/riseup_changingsettings#4.3)  
[81] <https://mail.riseup.net>  
[82] <https://help.riseup.net/security>  
[83] <mailto:ssayyed@riseup.net>  
[84] <https://mail.riseup.net/>  
[85] <http://roundcube.net/>  
[86] [https://info.securityinabox.org/tr/firefox\\_main](https://info.securityinabox.org/tr/firefox_main)  
[87] <https://mail.riseup.net/sm/src/login.php>  
[88] <https://help.riseup.net/email/webmail/where-is-imp>  
[89] <https://help.riseup.net/email>  
[90] [https://user.riseup.net/forms/password\\_reset](https://user.riseup.net/forms/password_reset)  
[91] <https://user.riseup.net/>  
[92] [https://info.securityinabox.org/en/riseup\\_changingsettings](https://info.securityinabox.org/en/riseup_changingsettings)  
[93] [https://user.riseup.net/forms/new\\_user](https://user.riseup.net/forms/new_user)  
[94] [https://info.securityinabox.org/en/riseup\\_createaccount](https://info.securityinabox.org/en/riseup_createaccount)  
[95] [https://info.securityinabox.org/riseup\\_createaccount](https://info.securityinabox.org/riseup_createaccount)  
[96] <https://info.securityinabox.org/sbox/screen/riseup-en-1/35.png>  
[97] <https://help.riseup.net/en/email/webmail#troubleshooting-webmail-login>  
[98] <https://help.riseup.net/en/email#frequently-asked-questions-faq>  
[99] <http://www.pidgin.im/download/windows/>  
[100] <https://otr.cypherpunks.ca/index.php#downloads>  
[101] <http://www.pidgin.im>  
[102] <https://otr.cypherpunks.ca/>  
[103] <https://info.securityinabox.org/en/jitsi>  
[104] <http://www.miranda-im.org/>  
[105] <http://adium.im/>  
[106] <http://dashboard.aim.com/aim>  
[107] <http://www.apple.com/support/bonjour/>  
[108] <http://komunikator.gadu-gadu.pl/>  
[109] <http://www.google.com/talk/>  
[110] <http://www.icq.com>  
[111] <http://www.msn.com/>  
[112] <http://www.mxit.com/>  
[113] <http://www.myspace.com/guide/im>  
[114] <http://silcnet.org/>  
[115] <http://www.ibm.com/developerworks/downloads/ls/ls/1/>  
[116] <http://messenger.yahoo.com/>  
[117] <https://info.securityinabox.org/sbox/programs/pidgin.exe>  
[118] <https://info.securityinabox.org/sbox/programs/pidgin-otr.exe>

[119] [https://info.securityinabox.org/en/riseup\\_main](https://info.securityinabox.org/en/riseup_main)  
[120] [https://jitsi\\_account#2.2](https://jitsi_account#2.2)  
[121] <https://jitsi.org/Register/Register>  
[122] <mailto:terencethetester@riseup.net>  
[123] [http://portableapps.com/apps/internet/pidgin\\_portable](http://portableapps.com/apps/internet/pidgin_portable)  
[124] <http://sourceforge.net/projects/portableapps/files/Pidgin-OTR%20Portable/Pidgin-OTR%20Portable%203.2%20Rev%202/>  
[125] [https://info.securityinabox.org/en/pidgin\\_main](https://info.securityinabox.org/en/pidgin_main)  
[126] <https://info.securityinabox.org/sbox/programs/PidginPortable.exe>  
[127] [https://info.securityinabox.org/sbox/programs/Pidgin-OTR\\_Portable.exe](https://info.securityinabox.org/sbox/programs/Pidgin-OTR_Portable.exe)  
[128] <https://info.securityinabox.org/tr/tr/glossary%23FOSS>  
[129] <https://info.securityinabox.org/tr/glossary#OTR>  
[130] <https://jitsi.org/Main/Download>  
[131] <https://jitsi.org/>  
[132] <https://adium.im/>  
[133] <https://guardianproject.info/apps/chatsecure/>  
[134] [https://info.securityinabox.org/en/Gibberbot\\_main](https://info.securityinabox.org/en/Gibberbot_main)  
[135] <http://www.linphone.org/>  
[136] [https://info.securityinabox.org/en/firefox\\_addons#3.2](https://info.securityinabox.org/en/firefox_addons#3.2)  
[137] [https://www.java.com/tr/download/help/disable\\_browser.xml](https://www.java.com/tr/download/help/disable_browser.xml)  
[138] <https://info.securityinabox.org/en/handsonguides>  
[139] <https://info.securityinabox.org/sbox/programs/jitsi.exe>  
[140] <https://jitsi.org/Documentation/RegistrarlessSIPAccount>  
[141] <https://support.google.com/accounts/answer/180744?hl=tr>  
[142] <https://support.google.com/accounts/answer/185833?hl=tr>  
[143] <https://xmpp.net/directory.php>  
[144] <http://xmpp.org/xmpp-software/servers/>  
[145] <http://www.process-one.net/en/ejabberd/>  
[146] <http://prosody.im/>  
[147] <https://www.riseup.net/en/chat>  
[148] <https://jit.si>  
[149] <https://xmpp.net/index.php>  
[150] [https://ostel.co/users/sign\\_up](https://ostel.co/users/sign_up)  
[151] <https://www.facebook.com/username>  
[152] <https://www.facebook.com/help/329992603752372/>  
[153] <http://windows.microsoft.com/tr-tr/windows/show-hidden-files#show-hidden-files=windows-7>  
[154] <http://itsfoss.com/hide-folders-and-show-hidden-files-in-ubuntu-beginner-trick/>  
[155] <https://info.securityinabox.org/en/glossary#OTR>  
[156] <https://info.securityinabox.org/en/glossary#encryption>  
[157] <https://info.securityinabox.org/en/chapter-3>  
[158] <https://info.securityinabox.org/tr/glossary#PGP>  
[159] <ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.18.exe>  
[160] <https://www.mozilla.org/tr/thunderbird/>  
[161] <http://enigmail.net/download>  
[162] <ftp://ftp.gnupg.org/gcrypt/binary/>  
[163] <https://addons.mozilla.org/en-us/thunderbird/addon/torbirdy/>  
[164] <http://www.mozilla.com/tr/thunderbird/>  
[165] <http://enigmail.net/>  
[166] <http://www.gnupg.org/>  
[167] <https://trac.torproject.org/projects/tor/wiki/torbirdy>  
[168] <http://www.claws-mail.org/>  
[169] <http://sylpheed.sraoss.jp/en/>  
[170] <http://www.washington.edu/alpine/>  
[171] [https://info.securityinabox.org/tr/gpg4usb\\_portable](https://info.securityinabox.org/tr/gpg4usb_portable)  
[172] [https://info.securityinabox.org/tr/riseup\\_createaccount](https://info.securityinabox.org/tr/riseup_createaccount)  
[173] <https://info.securityinabox.org/sbox/programs/tr/Thunderbird-en.exe>  
[174] <https://info.securityinabox.org/sbox/programs/enigmail.xpi>  
[175] <https://info.securityinabox.org/sbox/programs/gnupg-w32cli-1.4.x.exe>  
[176] <https://info.securityinabox.org/sbox/programs/torbirdy.xpi>  
[177] [https://info.securityinabox.org/tr/thunderbird\\_security#3.3](https://info.securityinabox.org/tr/thunderbird_security#3.3)  
[178] [https://info.securityinabox.org/tr/thunderbird\\_security](https://info.securityinabox.org/tr/thunderbird_security)  
[179] [https://info.securityinabox.org/en/avast\\_main](https://info.securityinabox.org/en/avast_main)  
[180] [https://info.securityinabox.org/en/comodo firewall\\_main](https://info.securityinabox.org/en/comodo firewall_main)  
[181] [https://info.securityinabox.org/en/spybot\\_main](https://info.securityinabox.org/en/spybot_main)  
[182] <https://info.securityinabox.org/tr/chapter-1>  
[183] [https://info.securityinabox.org/tr/firefox\\_others](https://info.securityinabox.org/tr/firefox_others)  
[184] [https://info.securityinabox.org/tr/avast\\_main](https://info.securityinabox.org/tr/avast_main)  
[185] [https://info.securityinabox.org/tr/thunderbird\\_encryption](https://info.securityinabox.org/tr/thunderbird_encryption)  
[186] [http://tr.wikipedia.org/wiki/Açık\\_anahtarlı\\_şifreleme](http://tr.wikipedia.org/wiki/Açık_anahtarlı_şifreleme)  
[187] [http://portableapps.com/apps/internet/Thunderbird\\_portable](http://portableapps.com/apps/internet/Thunderbird_portable)  
[188] [http://portableapps.com/support/thunderbird\\_portable#encryption](http://portableapps.com/support/thunderbird_portable#encryption)  
[189] <https://www.enigmail.net/download/>  
[190] <https://info.securityinabox.org/sbox/programs/ThunderbirdPortable-en.exe>  
[191] [https://info.securityinabox.org/sbox/programs/GPG\\_for\\_Thunderbird\\_Portable\\_1.4.11.paf.exe](https://info.securityinabox.org/sbox/programs/GPG_for_Thunderbird_Portable_1.4.11.paf.exe)  
[192] [https://info.securityinabox.org/tr/tor\\_main](https://info.securityinabox.org/tr/tor_main)  
[193] [https://info.securityinabox.org/en/tor\\_main](https://info.securityinabox.org/en/tor_main)  
[194] <https://www.mozilla.org/tr/firefox/new/>  
[195] <https://addons.mozilla.org/en-US/firefox/addon/noscript/>  
[196] <https://addons.mozilla.org/en-us/firefox/addon/adblock-plus/>  
[197] <https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/>  
[198] <https://addons.mozilla.org/en-US/firefox/addon/beef-taco-targeted-advertising/>  
[199] <https://www.eff.org/https-everywhere>  
[200] <https://www.google.com.tr/chrome/browser/desktop/>  
[201] <http://www.opera.com/tr>  
[202] [https://info.securityinabox.org/en/firefox\\_noscript](https://info.securityinabox.org/en/firefox_noscript)  
[203] <http://www.virustotal.com/>  
[204] <http://onlinelinkscan.com/>  
[205] <http://www.phishtank.com/index.php>

[206] <http://safeweb.norton.com/>  
[207] <http://www.urlvoid.com/>  
[208] <https://info.securityinabox.org/sbox/programs/Firefox-en.exe>  
[209] <https://info.securityinabox.org/sbox/programs/noscript.xpi>  
[210] <https://info.securityinabox.org/sbox/programs/adblock-plus.xpi>  
[211] <https://info.securityinabox.org/sbox/programs/better-privacy.xpi>  
[212] <https://info.securityinabox.org/sbox/programs/beef-taco.xpi>  
[213] <https://info.securityinabox.org/sbox/programs/https-everywhere.xpi>  
[214] [https://info.securityinabox.org/tr/firefox\\_portable](https://info.securityinabox.org/tr/firefox_portable)  
[215] [https://info.securityinabox.org/tr/keepass\\_main](https://info.securityinabox.org/tr/keepass_main)  
[216] <https://addons.mozilla.org/>  
[217] <https://www.mozilla.com/plugincheck>  
[218] [https://www.java.com/en/download/help/disable\\_browser.xml](https://www.java.com/en/download/help/disable_browser.xml)  
[219] [https://www.java.com/en/download/help/uninstall\\_java.xml](https://www.java.com/en/download/help/uninstall_java.xml)  
[220] <chrome://adblockplus/content/ui/firstRun.html>  
[221] <https://addons.mozilla.org/en-us/firefox/addon/cryptocat/>  
[222] <https://crypto.cat/>  
[223] <https://addons.mozilla.org/en-us/firefox/user/disconnect/>  
[224] <https://www.disconnect.me/>  
[225] <https://addons.mozilla.org/en-US/firefox/addon/duckduckgo-ssl/>  
[226] <https://duckduckgo.com/>  
[227] <https://addons.mozilla.org/en-us/firefox/addon/vtzilla/>  
[228] [https://securityinabox.org/en/avast\\_main](https://securityinabox.org/en/avast_main)  
[229] <https://www.virustotal.com/en/documentation/browser-extensions/>  
[230] <https://addons.mozilla.org/en-us/firefox/addon/sharemenot/>  
[231] <http://sharemenot.cs.washington.edu/>  
[232] <https://addons.mozilla.org/en-US/firefox/addon/clickclean/>  
[233] [https://securityinabox.org/en/ccleaner\\_main](https://securityinabox.org/en/ccleaner_main)  
[234] [http://portableapps.com/apps/internet/firefox\\_portable](http://portableapps.com/apps/internet/firefox_portable)  
[235] <https://info.securityinabox.org/sbox/programs/FirefoxPortable-en.exe>  
[236] <https://www.torproject.org/easy-download.html.en>  
[237] <https://www.torproject.org/projects/gettor.html>  
[238] <https://www.torproject.org/>  
[239] <https://help.riseup.net/en/riseup-vpn/>  
[240] <http://www.psiphon3.com/>  
[241] <http://www.dit-inc.us/freerate>  
[242] <http://www.your-freedom.net/>  
[243] [https://info.securityinabox.org/tr/firefox\\_noscript](https://info.securityinabox.org/tr/firefox_noscript)  
[244] [https://info.securityinabox.org/tr/firefox\\_others#5.1](https://info.securityinabox.org/tr/firefox_others#5.1)  
[245] <https://info.securityinabox.org/sbox/programs/tor-browser-en.exe>  
[246] <https://bridges.torproject.org/>  
[247] <https://check.torproject.org>  
[248] <http://www.iplocation.net/>  
[249] <http://www.ip2location.com/>  
[250] <http://whatismyipaddress.com/>  
[251] [https://info.securityinabox.org/tr/chapter\\_1\\_4](https://info.securityinabox.org/tr/chapter_1_4)  
[252] [https://info.securityinabox.org/tr/tor\\_anonymitynetwork](https://info.securityinabox.org/tr/tor_anonymitynetwork)  
[253] <https://www.torproject.org>  
[254] <https://www.torproject.org/about/contact.html.en>  
[255] <https://www.torproject.org/docs/faq>  
[256] <https://info.securityinabox.org/tr/chapter-9>  
[257] <http://joindiaspora.com>  
[258] <https://securityinabox.org/en/context/01/crabgrass-online-collaboration>  
[259] <http://friendica.com/>  
[260] <https://pidder.com>  
[261] <http://secushare.org>  
[262] <http://socialswarm.net>  
[263] <http://tosdr.org>  
[264] <http://www.facebook.com.tr>  
[265] <https://www.facebook.com/legal/terms>  
[266] <https://www.facebook.com/about/privacy/>  
[267] <https://www.facebook.com/help/privacy>  
[268] [https://info.securityinabox.org/tr/Tor\\_main](https://info.securityinabox.org/tr/Tor_main)  
[269] <https://info.securityinabox.org/en/chapter-7>  
[270] <https://www.twitter.com>  
[271] <https://www.twitter.com/tos>  
[272] <https://www.twitter.com/privacy/>  
[273] [https://info.securityinabox.org/tr/chapter\\_7\\_1](https://info.securityinabox.org/tr/chapter_7_1)  
[274] <https://transparency.twitter.com/>  
[275] <https://info.securityinabox.org/en/chapter-10>  
[276] [https://info.securityinabox.org/tr/Facebook\\_main](https://info.securityinabox.org/tr/Facebook_main)  
[277] <https://info.securityinabox.org/tr/chapter-11>  
[278] <https://www.youtube.com/>  
[279] <https://info.securityinabox.org/chapter-9>  
[280] <https://www.youtube.com/t/terms>  
[281] <https://www.google.com/intl/en/policies/privacy/>  
[282] <https://www.google.com/transparencyreport/traffic/>  
[283] [https://info.securityinabox.org/tr/firefox\\_others#5.5](https://info.securityinabox.org/tr/firefox_others#5.5)  
[284] [https://info.securityinabox.org/en/firefox\\_main](https://info.securityinabox.org/en/firefox_main)  
[285] <https://info.securityinabox.org/tr/glossary#Android>  
[286] [https://info.securityinabox.org/tr/glossary#guardian\\_project](https://info.securityinabox.org/tr/glossary#guardian_project)  
[287] <https://guardianproject.info/apps/informacam>  
[288] [https://info.securityinabox.org/tr/orbot\\_main](https://info.securityinabox.org/tr/orbot_main)  
[289] <http://support.google.com/youtube/bin/static.py?hl=en&guide=1388381&page=guide.cs&answer=2640535>  
[290] <https://www.vimeo.com>  
[291] <https://secure.flickr.com/>  
[292] <https://www.flickr.com/atos/>

[293] <https://info.yahoo.com/privacy/us/yahoo/flickr/details.html>  
[294] <http://privacy.yahoo.com>